ブロックチェーン技術の法的問題に関する一考察：仮想通貨を中心として

■論 説■

ブロックチェーン技術の法的問題に関する一考察
― 仮想通貨を中心として ―*

石　尾　賢　二

はじめに―ネットワークの現状

Web 2.0 とは、2000年代以降、情報の送り手と受け手が固定され、送り手から受け手への一方的な流れであった従来の状態が、送り手と受け手が流動化し、誰でもがウェブを通して情報を発信できるように変化したことに伴う様々な変化を言う。(1)

具体的には、ソフトウェアを開発し、サーバが中心となって利用する時代（クライアント・サーバ型ネットワーク（以下C/S と略する））、その後、個人・企業が巨大サーバの持つデータセンターを利用する（クラウドサービス―オープンソース、オープンデータ、ファイル共有など）ことができるようになり（巨大サーバ（プラットフォーム企業）のさらなる巨大化)、さらにピアツーピアネットワーク（以下、P2P と略する）を利用する時代へと変化する（同様にオープンソース、オープンデータ、ファイル共有などを利用するが、プラットフォーム企業に依存しないことが可能である)。これらの変化がどのような社会変化をもたらすのか、巨大なプラットフォーム企業がビッグデータと AI によってさらに巨大化するのか、個人によるインターネットの民主的な運営が発展するのか（例えば、シェアリングエコノミーはどのように発展していくのか）が問題となる。

そのような中でブロックチェーン技術を用いるビットコインが P2P においてノードを利用して通貨として流通する。ビットコイン等仮想通貨がネットワーク参加者間の決済手段として認知されている（平成28年資金決済法改正は仮想通貨取引業者を登録制とし、①：名義貸しの禁止（資金決済法63条の７）②：情報の安全管理（同法63条の８）③：委託先に対する指導（同法63条の９）④：利用者の保護等に関する措置（誤認防止等のための説明・情報提供義務）（同法63条の10）⑤：利用者財産の分別管理義務（同法63条の11）⑥：指定仮想通貨交換業務紛争解決機関との契約締結義務等（同法63条の12））を規定する。)。資金決済法は IT の発展に伴う資金移動に関するイノベーションの促進、利用者保護を目的とする法律であり、仮想通貨交換業に対する

規制が置かれた。

ビットコインなど仮想通貨の法的問題として二つの問題が区別される。一つはブロックチェーンの問題である。ブロックチェーンは「時間の経過とともにその時点の合意が覆る確率が０へ収束するプロトコル、またはその実装」(2)であり、主にP2Pにおいてユーザー認証された個人の暗号を利用した記載のある共有台帳を改ざんについての民主的な検証を経てブロックとして継続していくシステムである（実質ゼロ・ダウンタイムシステム）。このシステムは共有台帳記載の改ざんのないことが計算上保障されるために、台帳記載を訂正することが困難である。ブロック記載については、意思表示理論が当てはまり（意思表示の問題としては事業者・消費者間のブロック記載について消費者保護が適用困難という問題がある）、無効・取消とされうるのであるが、記載の訂正は困難である。その際、事前にブロックを承認しない方法、事後にハードフォーク（システムの仕様の変更による分岐が、新旧システム間で互換性のないように行われること）を行う方法などによって正しさが保障されうる。そして当初のブロック運営プログラムによる訂正方法、その後のブロック運営の改善方法の問題がある（第一の問題）。意思表示であるブロック記載の無効・取消の是正方法がプログラムによる事前処理あるいはハードフォークであり（当事者間での回復は別として）、それは民主的に行われる、あるいは管理者（プラットフォーム企業）が行う。第一の問題はシステムの問題であり、コンピュータ技術の問題と契約理論の問題がかかわり、技術優先の考え方と社会的妥当性の考え方がある意味で対立し、技術優先の考え方は自ら落ち度ある行為のために技術の安全性を危険にすることを認めず、過度の取引安全をもたらしうるものである。この技術優先の問題を参加者の同意の問題としてとらえることができるかが問題となる（プラットフォームの独占性の問題もある）。

ブロックチェーンは仮想通貨において多くを利用されるのであるが、二つ目の問題は通貨としての問題である。仮想通貨は私的通貨、私的金融として発展性も認められる（公的にも利用されうる）ものの、架空な価値を創設しうるために詐欺的利益取得、価格の乱高下等、架空性のもたらす危険性の大きなシステムである。(3)

仮想通貨とは、P2Pにおける共有台帳にネットワーク内での利用のために作成された記号通貨（デジタル通貨）であり、ネットワーク参加（ウォレット作成）に対する認証と当事者本人性を保障する暗号技術（当事者のみが持つ鍵で復号される）と改ざんされないことを保障するプルーフオブワーク（PoW）等を伴うブロックチェーン技術を用いるものであり、法定通貨の裏付けはないものの法定通貨と交換しうるものとなり、それ自体商品として取引されうるものである（取引所を経由するとこれらの手続きを取引所が主導する―クレジットカードと結び付けることを含めて）。仮想通貨には多様なものがあり、必ずしも一般に流通しないものもある。自らプログラム

を作成することもできるが、仮想通貨用のオープンソースのプログラム（GitHub など）、CounterParty などで独自トークンを発行する、イーサリアム上などでイーサとトークンの交換という形で作成することもできる(4)（GitHub の Microsoft による買収が発表されている(5)）。共通の価値認識に基づく交換媒体としてネットワーク内で一定の記号（トークン）を用いることができるのはもちろんであり（ゲームコインなど）、仮想通貨はブロックチェーン技術による記載の正しさに基づき一定の金銭（法定通貨）価値を有することになったものであり、売買対象となり、金融商品となりうる。したがって、仮想通貨に通貨として、金融商品として、企業金融としてどのような規制を置くのか（ネットワーク当事者間での通貨の作成とその内容と利用の拡大の問題、その金融商品としての問題）が第二の問題である。

本稿では、ネットワーク技術優先による自己責任システムはどこまで認められるのか、私的通貨に対する規制はどのようなものか、この二つの問題のうち第一の問題をインターネットの発展性において考察する。中心となるのは、仮想通貨におけるハッキング、マネー・ローンダリング等に対して管理者の権限強化が必要と考えられるが、その場合、現在のプラットフォーム企業と同様となるのか、個人の権利強化による民主的発展が可能であるのかという問題である。

一　ブロックチェーンとは

1．ブロックチェーン

ブロックチェーン技術は P2P において高い信頼性をもたらす台帳共有技術（分散型台帳技術）であり（複数台帳の更新の時間差を利用する二重払い等が防止される）、集団で管理される（ビットコイン取引ではプログラムに基づき約10分ごとに共有台帳の内容の正しさ・改ざんのないことが検証され、承認され、次ブロックが作成され、継続されていく）。このために、サービス提供者と受け手の分かれる C/S と異なり、すべての構成員がデータを保持することによるデータの安定性がもたらされ、セキュリティ対策費用の軽減がもたらされ、さらにブロックの改ざんを困難にする PoW などブロック検証が行われ、参加者の合意に基づき運営されうる（民主的運営）。このように、P2P は、今までの C/S におけるサーバ中心のインターネット取引（中央集権型）に対して、新たな民主的なネットワークビジネス（自律分散型）を可能にし、そのことはブロックチェーンによる改ざんされない安全な共有台帳を基本とすることで発展しうるのである。

ブロックチェーン技術を伴う P2P において、直接送金、海外送金に便宜であること、個人の需要・供給を直接結び付けることができ（宿泊、タクシー、マーケットプレイス、自家発電電力利用）、さらに金融面でのクラウドファンディングなどについ

て利用可能性が言われ、また、トレーサビリティの便宜から、IoT、ダイヤモンドなど高額物品管理、自動契約執行についての利用可能性、著作権管理に対する便宜も言われる。(6) これらの場合に直接当事者間のやり取りを同様の取引、あるいは個々の目的物についての取引をすべて共通台帳の上で行うことで、個々のニーズを満たす、共通の目的を達成する、継続的管理を可能にすることができ、スピーディーな契約を可能にし、車での移動や宿泊に関する民間での需給をマッチングさせるなど、小需要の発掘など小規模ビジネスの発展がもたらされうる。さらにはスマートコントラクトとして継続的な需給に基づき自動的に契約が執行されるシステムが行われうる。これらの記載は検証され、改ざん不能である。この場合のデータ更新は通常は管理者が行うと考えられる。

貿易取引において、輸出者、輸入者、銀行、保険会社、運輸会社、通関会社、税関、輸出入監督官庁等がかかわる中で、分散型台帳を用いると、「関係者に等しく情報が伝達され、仲介者を介さず、直接情報の参照や修正ができ」、修正についても、「記録がブロックチェーン上に残るので、何か不正があったとしても、過去に遡って検証できる」。(7)

２．前提としての仮想通貨流出問題

第一の問題についてはコインチェックの仮想通貨流出問題が問題点を明確にする。そもそもP2Pにおける分散型台帳（構成員が台帳記載を共有していく）では自己記載の改ざん、不当記載（台帳自体の瑕疵－例えば時間的ずれを利用した二重記載）、その他台帳共有化過程での改ざんが重要な問題であったが（内容面は一定のプログラム上のチェックが可能である）、PoW等を伴うブロックチェーンを用いることによってブロックの改ざんがほぼ認められないことになり（改ざんにより承認された数値が変更されてしまう）、このことはチェック回数を増やすことによってより確実となる。ただし、個人のハッキングによるなりすまし（ハッキングされた個人の過失）は可能であり、コインチェック流出問題は取引所のハッキングによる個人の仮想通貨の流出である（取引所、個人の双方に過失あり）。この問題において、流出したネムは特定され、追跡可能であるが、取り戻せない、無効化できない。ネム財団はハードフォークによる無効化が可能であったが、全体にかかわることであり、全体の価値・今後の取引価値を考え、行わなかった（ハッキングによる被害を是正するよりも日本の取引所のミスの問題とする方が良いと考える）。(8) 同様のDao事件でイーサリアムはハッキング以前の状態に戻すハードフォークを多数の賛同により行ったが、このような中央集権的処理への反発から分裂が生じた。(9) このようにハードフォークは様々な可能性を有するが、誰がハードフォークを行う権限を持つことができるのか、全員の合意により行う場合にはそのような管理をスムーズに行うことは可能かなどの問題を有す

る。そもそもそのブロックを承認しなければブロックが有効となることはなかったのであるが、ネムの Proof of Importance（PoI- コインの保有量、取引頻度による重要な参加者が承認する権利を持つ仕組み）は承認した（迅速な承認も仮想通貨運用の価値の一つではある）。承認は基本的にはマイニングの計算結果についてであるが、それ以前にプログラムが内容チェックを要求し、プログラムによってはより詳細な事前チェックも可能である。基本的に多数者の承認により不正なブロックの存続が認められうる。このようにまずシステムの問題としてブロックの承認方法、承認したブロックを訂正できないこと、ハードフォークによるやり直しが問題となる。

また、コインチェック流出問題において、仮想通貨取引所（取引相手を見つける、法定通貨との交換を媒介するなどを行う）は免責条項を規定するが、補償に応じている。仮想通貨取引は取引所を経由しなくても可能であるが、多くの場合は取引所を経由し、個人は取引所にウォレットを置き、取引所にログインすることによってデジタル署名を用いて取引を行うこととなっている。この場合に取引所と個人の責任分担の問題が生じる。

このようにブロックチェーンはブロック記載に改ざんがないこと、不正なブロック記載を追跡しうることが重要な特色であり不正取引の扱いについては更新の際に承認を行わない、ハードフォークを実施することを多数決で行う、管理者が行うなどの方法が考えられるが、基本的な性質として適正かつ迅速なプログラム処理と迅速なチェックが重視され、取引安全をもたらすものであり、訂正・修正を基本的に認めないことが挙げられる（参加者の自己責任が重視される）。参加者各人が台帳を共有し、自己責任において記載し、合意事項に基づき管理し、管理方法に基づき台帳が更新され、台帳は訂正できない。

二　P2P とブロックチェーン

1．P2P とは

「C/S モデルでは、データを保持し提供するサーバとそれに対してデータを要求・アクセスするクライアントという 2 つの立場が固定されているのに対し、P2P は各ピアがデータを保持し、他のピアに対して対等にデータの提供および要求・アクセスを行う自律分散型のネットワークモデル」である。(10) P2P とは、「ネットワークに参加しているコンピュータがそれぞれ同等の立場を持ち、平等で、特別なノードがなく、すべてのノードがネットワークサービスを提供する負荷を分担していることを意味」する。(11) このように P2P では階層的ではなく、フラットな性質を持ち、多数の個人が直接関わる仕組みを構築することができる。

「P2P の分類として、データの所在を一括保持するサーバを持つハイブリッド

P2P、そのようなサーバを持たないピュア P2P、処理能力の高いノードが自発的にデータの所在を探索・保持するスーパーノード型 P2P が」ある。(12) ハイブリッド P2P、スーパーノード型 P2P ではインデックス・サーバ、スーパーノードがデータを管理することができ、ピュア P2P では各人が管理する。個々の障害は全体に影響しない。「ビットコインのノードは、ルーティング、ブロックチェーンデータベース、マイニング、ウォレットという機能の集合体」であり、 4 つすべて持つものがフルノードである（一部のみ持つ SPV ノードもある）。(13)

P2P には、常時動作している基本ネットワークと必要な時に当事者間で行うダイナミック P2P アクセスがある。

「実用化されたシステムとしては P2P データ配信、P2P 電話、P2P 掲示板、P2P 放送（テレビ、ラジオ）、P2P グループウェア、P2P 分散ファイルシステム、P2P-SIP、P2P-DNS、P2P- 仮想ネットワーク、P2P 地震情報などがある。またここ数年、商用的にも注目を集めており、特に IP 電話（Skype, LINE など）や動画配信サービス（Veoh など）といった応用例が増えてきている。」(14)

利用者間で音楽ソフトを無料で交換することを可能にするファイル共有ソフト（Napster）を持つ者の間のネットワーク、Skype を利用して電話通信を行うネットワークなど、P2P は対応ソフトを持つ者同士間の通信、対応ソフトを持つ者同士の共有ファイルの利用に用いられてきた。Skype は、アプリケーションをインストールし、Skype Account Manager（サーバ）にユーザー登録し、ログイン認証によってスーパーノードを通して利用する（同期型）。(15) 非同期型の中で広範囲流通 Contents Delivery Network（CDN）の中で、BitTorrent は、BitTorrent クライアントをインストールし、欲しいデータの torrent ファイルをダウンロードし、要求すると自動的に Tracker に問い合わせ、各ノードから欲しいデータを取り寄せる。(16)

「P2P モデルで通信を行うファイル共有ソフトが、トラフィックを増加させたり、自分が著作権を持たないファイルを違法に交換することに使われたり、共有されているファイルなどを不用意に開いてしまい、それが原因でウィルスなどに感染してしまった結果、情報漏洩などを引き起こしてしまうなどといった負の影響が」あり、「その一方、サーバへのトラフィックおよび負荷集中を避けられる、単一障害点がない（ピュア P2P の場合のみ）などの利点のため、ファイル交換だけではなく VoIP（Voice over IP）、IM（Instant Messaging）、グループウェアなどファイル交換を主としない用途でも使われ」る。(17)

ファイル共有は著作権の問題を多く生じさせる（Napster、Winny など）が、参加者全員が協力し合うシステムにおいて、データを共有することは著作権侵害となるものもあると考えられるが、私的使用の範疇にあるものはならない、あるいは認められうる中古品流通にあたる場合はならない。自らオープンソースとするソフトウェア

も公開されている。

著作物の権利者が、だれでもが無償で自由にアクセスできるサイト上へ情報を掲示し、当該サイトにアクセスする者すべてが自由に閲覧することを許容している場合、サイト上の情報をディスプレー上ではなく紙面上で閲覧するためにプリントアウトするという複製行為について禁止する旨の特段の意思表示がない場合には、多くの場合、権利者から黙示の許諾があると認められるものと考えられる。(18)

平成21年に著作権法が改正され、一定の場合に著作物を著作権者の許諾なく利用しても著作権侵害とならないことを定める権利制限規定が整備され、違法な著作物の流通の抑止規定が置かれ（平成24年刑事罰規定)、平成22年１月１日から施行されている。同改正によって新設された著作権の権利制限規定のうち主なものは以下のとおりである（その後平成24年・26年・30年に改正される)。

情報検索サービス事業者がそのサービスの提供過程において、インターネット上に公開された情報の収集、整理及び検索結果としての提供を行うために記録媒体への記録、翻案及びURLの提供と併せて公衆送信を行うことができる（著作権法第47条の６、同法施行令第７条の５、同法施行規則第４条の４)。情報検索サービスが著作物の流通促進等一定の社会的基盤としての意義を有しており、また、公正な手続きに則って提供される情報検索サービスについては、その過程で行われる著作物等の利用行為が著作権者に与える不利益は少ないと考えられることから著作権の権利制限の対象となったものである。サーバでの情報蓄積も著作権侵害ではない（47条の５)。インターネット販売等での美術品等の画像掲載、情報解析のための抽出、統計的な処理等を行うために記録媒体への記録、翻案を行うことも無許諾で可能とされる（著作権法第47条の２・第47条の７)。著作権者不明の場合の利用円滑化も図られる。(19)

P2Pのメリットとして、高スケーラビリティ、低コスト、高耐障害性、匿名性が言われる。デメリットとして、様々なPCが対象であり、参加脱退の激しいノードがいるために実装が困難であること、動作確認が困難であること、データの消除が困難であること、セキュリティ制御が困難であること、インターネットの負荷が大きいこと、通信相手の特定が困難であることなどがあげられている。ただし、管理者を置くタイプでは一定のデメリットの軽減が図られうる。(20)

P2PではC/Sのようなサーバへのアクセス集中がない代わりに、すべてのピアが検索機能を有する共有システムを有するために、各参加者の負担が大きくなる。

C/Sはサーバが多大なセキュリティ負担を担いつつサーバの管理責任においてサイトを運営するシステムであり、これにより情報が集約化し、独占的な地位を築いていく。それに対して、P2Pは個々の参加者が対等に負担し、共同して問題に対処しうる。このP2Pがブロックチェーンを用い、データ改ざんを否定することによって仮想通貨利用が可能とされる。ブロックチェーンは改ざんのないことを証明するとと

もにその記録を残しておくことによって P2P の仕組みの精度を高める。

問題としてはサーバのような管理者のいない場合の運用である。P2P においても管理者のを置く方法もある（Airbnb, Uber）。

2．P2P におけるブロックチェーン利用例(21)

ブロックチェーンについては後に述べるが、信頼性を高めるブロックチェーン技術により P2P の発展がもたらされている。現在の大量生産、大量消費に対して、消費者のニーズに合わせた商品供給が可能となる。また、大量の中間業者を経由して大企業と取引をするのではなく、直接当事者間の取引となる。ロングテールである、ニッチである商品販売の拡大－人気商品の大量生産とは別にシェアリングエコノミー（物・サービス・場所などを、多くの人と共有・交換して利用する社会的な仕組み）が行われる―自律分散システム。さらに商品の追跡可能性を継続する。ICO などの金融（仮想通貨については後述）。(22) いずれも改ざんのないことは重要な要素であるが、それ以上に記載内容の正しさも問題となる（なりすましのないことも含めて）。

具体的な応用領域として、支払い、クリプトカレンシー、マイクロペイメント、デジタルアセット、デジタルアイデンティティ、公証サービス、税金、投票、記録管理が挙げられる。(23)

より具体的には、「①地域通貨・ポイント・電子クーポン、②土地登記・特許・文書管理・届出・投票、③サプライチェーン・貿易取引・貴金属・宝石管理・美術品真贋認証、④シェアリングエコノミー・CtoC・電子図書館・スマートロック（スマホなどで操作する鍵）・デジタルコンテンツ・チケット、⑤スマートコントラクト・遺言・エスクロー（第三者を介した取引）・会社清算・エネルギー管理・IoT」が挙げられ、それぞれ記録管理が行われる。(24)

(1) 需給の調整としての利用（シェアリングエコノミー）

シェアリングエコノミーとして有名なものに、Uber, Airbnb があるが、ブロックチェーンが利用されている。

(2) エネルギー利用の合理化

発電と電力消費の合理化としてブロックに個人消費電力と余剰電力が記載され、マッチングされる。個人の電力のニーズを直接把握することができるために、電力自由化のメリットが現実化するしくみを作ることができる。例えば小規模の地域の各戸が蓄電する、あるいは自家発電を行い、その中で「蓄電装置と電力融通ルーターなどによって」自律的に需給調整を行う。(25)

(3) 物の追跡

ブロックに記載された物に関する取引の過程をたどることができる。物の権利の証

明を確実にする。

IoT の活用による設計・開発、生産、販売、運用・保守における合理化が図られる。

「英 Everledger 社は、ダイヤモンドの形状をセンサーで読み取ってデジタル指紋に変換し、ブロックチェーンにダイヤモンドの認定書を記録。また、そのダイヤモンドが消費者に販売されるまでの取引ルートを追跡しブロックチェーンに記録することにより、消費者が盗品を購入してしまうことを防いでいる。」(26)

「食品供給は生産・加工・流通・販売の 4 段階に大きくカテゴライズされ、複数の関連業者の介入があり、ようやく消費者の元に産物が届く。そのため潜在的リスクの予想や分析が困難な状況だ。こうした不透明さの改善において、ブロックチェーン技術の『追跡性』が貢献すると期待されている。」「食品が生産者から出荷され、消費者の元に届くまでの経過をブロックチェーン上に細かく記録することで、サプライチェーン（供給網）の透明化を図る。」(27)

「オーストラリアのスタートアップ企業である Full Profile 社が提供している世界初のブロックチェーン・コモディティ・マネジメント・プラットフォーム『AgriDigital』」は「穀物の生産者（農家）と買い手、そしてサイト管理者が契約から配送、倉庫間の移動、請求、決済までの全プロセスを、単一のプラットフォーム上で行える」(28)「『AgriDigital』はリアルタイムで市場価格が追跡可能なため、農家は現在の市場価格を正確に把握し、最適な価格で取引を行える。希望出荷価格を設定しておけば、「今すぐに取引を行うか、あるいは時間をおいてから市場に流すために倉庫に保管するか」といった重要な意思決定にも大きく貢献する。「まずは買い手が希望仕入れ価格を入札する。売り手と買い手が合意に達し、取引が成立すると、プラットフォーム上で自動的に契約書が作成される。買い手には取引成立が通知され、合意に達した価格で請求書が発行される。」(29)

「RSPO は持続可能なヤシ油の生産・供給を市場で標準化するために、認証システムを導入した。農園での生産から流通までの各プロセスを管理下に置く。RSPO が定めた原則と基準を満たしていると保証するサプライチェーンや生産者に認証が発行され、製品には RSPO のトレードマークを表示する許可が与えられる。」(30)

Smart Containers グループは製薬会社と食品会社のコールドチェーンの問題（生産・輸送・消費の過程で途切れることなく低温を保つ物流方式）を解決し、スマートコントラクトによって全世界の人が低温物流サービスに参入・利用できるソリューションを実現しようとしている（ICO による資金調達も行っている）。(31)

「ブロックチェーン上のスマートコントラクトは、『コンピュータが読めるプログラムを書き、当事者双方の署名付きでブロックチェーンに登録することで、それを契約締結と見なし、法執行機関なく自動的に執行されるようにする』というアイデアである。ブロックチェーン上で契約と執行をプログラム化し、決まった形式ができると、

契約内容が自動で執行され、大幅な業務効率化につながる。」(32)

(4) 不動産登記など権利の証明、文書の証明等

「ブロックチェーン上に不動産情報を加えていくことで、過去の取引を含めた連続的な情報をスマートフォンなどの手元にあるデバイスから一括して取得することが可能となる。また、ブロックチェーンの活用によって、中央集権的な管理が不要となり、コスト削減や登記手続きの効率化にもつながる。さらには、不動産登記システムのセキュリティが高まり、不動産取引の安全性が向上する可能性もある。」(33)

不動産を小口化する際の問題対処も期待されている。「BrickBlock はブロックチェーン上に取引プラットフォームを構築し、不動産や ETF などの資産を管理する試みを行っている。高度な自動化とブロックチェーン技術、スマートコントラクトの使用により、決済機関や仲介業者など多くの第三者を不要にしようとしているのだ。そしてこれにより、資産の売買に関連する手数料を従来の仲介業者と比べて大幅に下げようとしたのである。」(34)

「Factom 社は、ブロックチェーンを使い文書の存在証明をさまざまな分野へ展開しようとしている。医療や保険といった分野での活用が期待されるほか、土地登記謄本といった権利書類の記録管理サービスを提供しており、中国政府が主導するスマートシティ計画に参画するとも言われている。」(35)

「豪 Flux 社はブロックチェーンをベースに選挙システムを構築し、市民の声を政治により反映しやすくさせようとする取り組みを行っている。」(36)

(5) 医療

個人医療データをブロックに蓄積していくことで、個人医療と共に他の参考となる医療のデータが共有される。

「個人情報から切り離された医療データを収集して解析するプラットフォームを世界中の医療関係者が共有することができれば、医師たちはこれまでにない知見を得ることができ、患者もより適切な治療を受けることができるようになるのは確かだ。そこで、個人情報を扱う医療プラットフォームとしての信頼を得るために、DeepMind はブロックチェーンを活用して暗号化した患者の個人情報をリアルタイムで追跡できる『Verifiable Data Audit』を2017年中に導入すると発表した。」「『Doc.ai』は、ブロックチェーンと人工知能を活用することで、グローバルに収集した大量の医療データから医師が洞察を得るための会話型プラットフォームである。個人ユーザーに対するサービスも提供しており、ディープラーニングによって解析されたデータを活用することで、彼らが抱えている健康上の悩みに対するフィードバックをすることも可能だ。」(37)

(6) フィンテック(38)

「金融と IT（情報技術）を融合した新サービスや、その新サービスを提供する事

業者。finance（金融）と technology（技術）を組み合わせた造語で、2008年のリーマン・ショック以降、アメリカを中心に発展した概念である。決済、融資、送金、資産運用・管理、会計、保険、仮想通貨、経営・業務支援など、これまで金融機関がほぼ独占していた金融サービスをインターネット、クラウド、スマートフォン、ビッグデータといったITを活用することで、より便利に、より低コストで、より迅速に提供しようという動き全般をいう。フィンテックには、(1)サービス対象を個人や中小企業に特化している、(2)従来、既存銀行の顧客ではなかった幅広い層に金融サービスを提供できる、(3)店舗や銀行・証券口座を介在しないサービスも多い、(4)金融と無縁であったITベンチャー企業などの多様な異業種が参入している、(5)銀行法などの従来の金融関連法制の規制を受けない、といった特徴がある。具体的には、スマートフォンなどモバイル機器を利用した電子商取引の決済サービスが相次いで登場しているほか、資金の貸し手と借り手をネット上で結びつける融資サービス、金融機関の個人口座を管理するサービスなどが収益を生み出している。またベンチャー・キャピタル市場では、フィンテック関連のベンチャー企業への投資や上場が関心を集めている。一方で、サイバー犯罪やマネー・ローンダリングに悪用されるおそれがあり、不正防止や資産の保護が課題となっている。

世界ではアメリカとイギリスがフィンテックの振興に積極的に取り組んでおり、日本でもメガバンクや地方銀行がIT企業と提携したりフィンテック対応部署を設けたりするなど、積極的にビジネスに取り入れ始めた。2016年（平成28）５月にはフィンテックを促進するための改正銀行法が成立した。」

(7) 金融等

「IBMとインドのマヒンドラ・グループが共同開発したブロックチェーン金融ソリューションは、資金の流動性やコスト削減などを図る、インドのサプライチェーン・ファイナンスの改革を目指して開発された。共有プラットフォームを通して、供給から製造までの全取引履歴に、全関係者がリアルタイムでアクセスできるため、ここで立証された信頼性と透明性に基づき、新たな第三者融資システムの構築などに役立てる案が出ている」(39)

「米Nasdaq社の未公開株式取引市場であるNasdaq Private Marketの『Nasdaq Linq』と名付けられたシステムだ。例えば株式未公開企業の従業員らが、自身で保有している株式を売買でき、その取引の『台帳』を実装する技術としてブロックチェーンを使用しているという。」(40)

「米国のベンチャーであるGyft Block社はブロックチェーンを活用して、ポイント交換システムを立ち上げており、安価で信頼性の高い、ギフトカードを交換する仕組みを作り出している。」(41)

(8) ICO

企業の資金調達として株式公開などの従来の方法が用いられてきたが、規制などが多いために、仮想通貨による資金調達方法が活用されている（トークンを売るだけ)。法定通貨に換算すると莫大な金額がトークンによって集められ、そのまま利用され、トークンの持ち主もそのまま利用する。ただし、詐欺による資金調達としても利用される。2017年の ICO 規制は以下である。 7 月にアメリカで認可を受けない ICO による資金調達は、証券取引法に基づく処罰の対象とされ、 8 月にシンガポール金融管理局（MAS）証券先物法の対象となる ICO の規制を発表、 9 月に中国金融当局によって、ICO で仮想通貨を利用した資金調達が禁止され、10月に韓国の金融規制当局は ICO 禁止を発表する。それにともない仮想通貨の信用取引も禁止。(42)

(9) 仮想通貨

そもそもブロックチェーンの安全性技術と民主制はビットコインを爆発的にヒットさせ、類似の仮想通貨（アルトコイン）が無数に作成されている（詳細は後述)。

3．P2P でのブロックチェーン利用の検討

P2P のブロックチェーン利用の検討項目については以下のように言われる。(43)

「ブロックチェーンを利用するための要件は満たされているか。利用されるブロックチェーンはどのような種類のものか。純粋な分散型の P2P システムを利用することの付加価値は何か。そのブロックチェーンアプリのアイデアはどのようなものか。ビジネスケースはどのようなものか。システムにリソースを提供することに対してピアはどのように補償されるか」。

ブロックチェーンを利用するための条件については以下のように言われる。(44)

「そのシステムのアーキテクチャは何か。システムコンポーネントは何か、それらのコンポーネントは互いにどのように接続されるか。純粋な分散型のシステムか。それとも、失敗するとシステム全体をダウンさせるような中央のコンポーネントが存在するか。新しいノードはどのような仕組みでシステムに参加するか。誰でもシステムに参加して、計算リソースで貢献することは可能か。新しいノードを対象とした何らかの新規参加プロセス、適正評価プロセス、または事前のセキュリティチェックが存在し、制御の中心となる要素が確立される可能性はあるか。そのシステムではすべてのノードが同じ役割と権利を持つか。それとも、データの読み取りと書き込みの権利はノードごとに異なるか」。

利用されるブロックチェーンの種類については以下のように言われる。(45)

「どのような種類のブロックチェーンが利用されるか（パブリックかプライベートか、許可型か非許可型か)。どのような権利が制限されるか。どのグループのノードにどの権利が与えられるか。その種類のブロックチェーンが選択されたのはなぜか。

どのグループのノードにどの権利を与えるか決定するのは誰か。システムにに対する読み取りアクセスと書き込みアクセスの許可または拒否に関するルールを決定し、適用するのは誰か。新規参加プロセスを実行するのは誰か。特定の権利を制限することが正当化されるようなプライバシーやスケーラビリティの問題はあるか」。

ブロックチェーンアイデアの内容については以下のように言われる。(46)

「そのブロックチェーンアプリの目的はそもそも何か。そのシステムの主な問題領域は何か。そのシステムを特定の産業セクターに関連付けることは可能か、可能であるとしたらその産業は何か。そのシステムがユーザーに提供するサービスはどのような種類のものか。そのシステムが利用するブロックチェーンの一般的な使用パターンは何か。そのアプリケーション領域にブロックチェーンの法的容認に関する問題はあるか。そのブロックチェーンに格納されるデータはどのような種類のものか。そのブロックチェーンで実行される操作やトランザクションはどのような種類のものか。そのブロックチェーンで利用されるセキュリティ機能はどのような種類のものか。これらの要素はブロックチェーンアプリのアイデアとどのように関連するか」。

三　ブロックチェーン技術

1．ブロックチェーン技術概要

ブロックチェーンとは分散型台帳技術の一つであり、取引データ等を中央管理（サーバ管理）ではなく、共有管理し、民主的運営を可能にするとともに内容と改ざんについて常時チェックし、承認・確定し、改ざんを困難にする仕組みである。(47)チェックはビットコインについてはマイニング（PoW －改ざんのないことを数値によってチェックする）によって報酬（新しいブロックを作成する数値を発見したときに与えられるビットコインと手数料）を伴って行われるが、その他の方法もある。

「ブロックチェーンは報酬と罰則の力によって完全性を達成する。報酬は手数料に基づく収入として実装され、罰則は『プルーフ・オブ・ワーク』として実装される」(48)

ブロックチェーンとは一つのブロックに「①一定期間ごとの多数の取引データ。②前ブロックのハッシュ値。③ナンス値と呼ばれる数字、の 3 つが含まれ」、それぞれのブロックを検証しながら、つなげていくシステムである。(49)

ビットコインでは、まずパソコンなどに Bitcoin Core などのブロックに参加するためにソフトウェアのインストールを行い、その後個々の取引がウォレットを通して本人確認（ユーザー認証）を経てブロックに記載され（暗号鍵を使いデータを暗号化し、復号する暗号鍵によって復号される―デジタル署名)、拡散過程でプログラム上の内容チェックがなされ、数値承認を伴う新たなブロック作成によって改ざんのないことが検証されるとともにビットコインが増加する。ウォレットには用途によって

ウェブ型（第三者（取引所）のウェブサービスを利用する―ログインアカウントによる利用）、デスクトップ型（ソフトウェア型）、モバイル型（ソフトウェア型）、ハードウェア型（電子データとして持ち歩き、接続によって利用）、ペーパー型（紙に保存）がある。(50) また、常時接続型のホットウォレット（ウェブ、スマホなど）とそうではないコールドウォレット（ハードウェア、ペーパー）がある。投機取引にはホットウォレット（セキュリティを取引所が管理するもの）が用いられるであろう。取引記載には送金額、送金人、受取人などの取引情報が含まれる。(51)

ビットコインにおける取引経緯を見る。

ビットコイントランザクションとは「ビットコイン所有者が他の人にビットコインを送ったと認めたことを、ビットコインネットワークに示すこと」である。(52)

トランザクションの借方にインプットが記載され、貸方にアウトプットが記載される。インプットの所有権の証明はデジタル鍵、デジタル署名によって行われ、他人によって検証される。個人とのつながりをもたらすデジタル鍵は、「ファイルやウォレットと呼ばれる単純なデータベースに保持されて」いる。(53)

ＡからＢへのビットコインによる支払いは、例えば、以下の手順で行われる。

Ａが現金と引換にビットコインを購入する。このトランザクションはＡの秘密鍵でロックされている（Ａのウォレットには通常Ａの未使用アウトプットが保持されている）。ＡからＢへのトランザクションは、Ａのビットコインの購入をインプットとして参照し、Ｂへの支払いとお釣りの受け取りをアウトプットとして作成する（手数料も差し引かれる）。トランザクションはチェーン形式であり、最新のトランザクションのインプットは前のトランザクションのアウトプットである。Ａの秘密鍵は前のトランザクションのアウトプットを解錠し、そのビットコインがＡのものであることをネットワークに示し、このビットコインをＢのアドレスに紐づける。このアウトプットを使用するためにＢは署名を作成する。その後、Ｂのパブリックアドレスに対応する秘密鍵から作られた署名を提示する人にこのアウトプットが支払われる。

ビットコインネットワークに伝えられたこのトランザクションは膨大な計算によるマイニングと呼ばれるプロセスを通して検証されブロックに取り込まれるまで、ブロックチェーンの一部となることができない。

すなわち、トランザクションはネットワークのノードにより未検証のトランザクションプールに入れられ、PoW による計算解が求められ、ブロックがつなげられていき、信頼度が高くなっていく（６回より多く検証されたブロックは改変できないとされる）。(54)

2．データ検証

以上、数値による民主的チェックが特色であるが、プログラム上内容の正しさもチェックされうる。

(1) ビットコインにおけるプログラムによるチェック

内容の正しさについて、例えばビットコインに関してはプログラム上以下のチェックが最初に受け取ったノードにおいて行われる。(55)

「トランザクションの構文とデータ構造は正しいか。インプットとアウトプットのいずれも空でないか。バイト単位のトランザクションデータサイズが MAX_BLOCK_SIZE よりも小さいか。それぞれのアウトプット value 及び total value は許されている値の範囲内（ 0 より大きく2,100万 bitcoin よりも小さい）にあるか。インプットのいずれも hash=0, N=-1 でないか（coinbase トランザクションはリレーされるべきでない)。nLockTime は INT_MAX より小さいかまたは等しいか。バイト単位のトランザクションデータサイズは100より大きいかまたは等しいか。トランザクションに含まれている署名オペレーション数は、署名オペレーション回数上限よりも小さいか。Unlocking script(scriptSig) はスタックに数字を push することだけしかできず、locking script（scripyPublkey）は isStandard 形式に合っているか（これにより「非標準」トランザクションは拒否される)。トランザクションプールまたはメインブランチブロックチェーンのブロックに。同じトランザクションがあるか。各インプットに対して、もしこのインプットが参照しているアウトプットをトランザクションプールの他のトランザクションも参照していた場合、このトランザクションを拒否する。各インプットに対して、メインブランチブロックチェーンかトランザクションプールにインプットが参照しているトランザクションアウトプットが見つかるかを確認する。もし参照しているアウトプットが見つからなければ、これはオーファン（孤児）トランザクションである。オーファントランザクションプールにまだこのトランザクションがなければ、オーファントランザクションプールにこのトランザクションを追加する。各インプットに対して、もしインプットが参照しているアウトプットが coinbase アウトプットだった場合、このアウトプットは少なくとも COINBASE_MATURITY（100）の承認数を待っているか。各インプットに対して、参照しているアウトプットがすでに使用されて使用不可になっていないか。参照しているアウトプットを使って、それぞれのインプット value とその総和が許されている値の範囲内（ 0 よりも大きく、2100万 bitcoin よりも小さい）にあるか。もしインプット value の総和がアウトプット value の総和よりも小さければ拒否する。もしトランザクション手数料が少なすぎて、空ブロックに入ることができない場合は拒否する。各インプットにある unlocking script は、対応したアウトプットの locking script を解除できるか」。

(2) ビットコインのコンセンサスアルゴリズム

次にブロック改ざんの有無が検証される。

ハッシュ値とは、ハッシュ関数により元のデータから得られる数値であり、少しでも異なるデータからは異なるハッシュ値となり、ハッシュ関数（圧縮関数を含む）は出力値から入力値を復元することのできない一方向性を有する。この数値の検証から、データ改ざんの実質的不能がもたらされる（改ざんにはすべてのデータを改ざんしなければならない）。(56)

「ブロック全体のデータは『前ブロックのハッシュ値＋取引データ＋ナンス値』から構成され」、ビットコインにおいては次のブロックに使うハッシュ値の条件を満たすナンス値が必要となる。このことは次ブロック作成による前ブロックに改ざんのないことの検証となる。(57)

ビットコインにおいては『前ブロックのハッシュ値＋取引データ＋ナンス値』から新規ブロックのハッシュ値を求め、そのために必要なナンス値を求めることになり、この膨大な計算によって10分ごとに求められたナンス値による次ブロック作成が取引の承認といわれる（PoW 当該ブロックのすべての取引が承認され、取引が確定する）。(58) 承認された後、以前の記録を改ざんできない。

ビットコインではこの次ブロックを作成するナンス値を求めること（PoW の実行）をマイニングといい、報酬が支払われる。マイニング報酬を求めて（複雑な計算をするとビットコインと手数料がもらえる－計算の実行によるブロック作成に伴うビットコインの発行）、マイナーたちがこれを行い、このことがデータの信頼性を検証する。(59)

ビットコインの偽造とはこの後のすべてのブロックの計算をやり直すことであり、実質的には不可能である。(60)

「ビットコインでは、このように、①暗号技術。②ブロックチェーン技術、③ PoW といった技術の組み合わせによって、安全な取引を可能に」する。(61)

ブロックチェーン技術は、改ざんの困難性を示すハッシュ値と継続的検証を示すナンス値の発見と承認により継続するデータの信頼性を民主的に検証する有用な方法である。

取引がブロックに記載されると、不特定多数のマイナーが PoW に参加し、ブロック記載を前ブロックと照合検証し、認証した記載を含む次ブロックを作成する。認証は二重払い、書き換え、不正残高など不正データ、不正処理に関するものであり、なりすましなどはチェックされない。PoW に成功したマイナーが現れると、その結果をほかのマイナーが検証し、誤っていた場合は改めて検証作業が開始し、成功した場合はそのマイナーが次ブロックを作成し、取引が確定し、そのマイナーに報酬が与えられる。報酬を期待するマイナーによる検証がデータの改ざんのないことを保証する。

このような方法によるデータの確実性はビットコインの価値を高めることにもなる（自主的検証による信頼性と P2P 利用の便宜性）。

分岐が生じた場合（二重使用）は多数継続する方が正しいものと判断される。

ただし51％のマイナーが悪意であった場合には検証が機能せず、間違ったブロックの継続がなされうる（51％攻撃）。マイナー寡占化の問題である。

「51％攻撃とは、ネットワークの51％の計算量を一部のマイナーが支配し、自分たちの都合のいいように新規ブロックをマイニングし、取引を操作」し、二重支払い、マイニング報酬独占（作成ブロックを隠し持っておく）などを可能にすることである。(62) 1/3以上の悪意の結託により正しい合意が形成されないとも言われる。

モナコインではマイナーが次ブロックを公開せず、記載を行い、最長となった時点で公開し、もともとのブロックの送出金記載を無効化して、二重に利益を得ることが行われた。(63)

(3) 他のコンセンサスアルゴリズム

以上の計算解をすべての関係者が求めることができ、コンピュータの性能により早く解を求めることができた者が報酬を得る仕組みがビットコインで用いられている PoW であるが、このようなコンピュータの能力に依存する仕組みとは異なる仕組みも作られている。特定の者が優先的に解を求めることができるとする仕組みもある。

PoS（Proof of Stake）では、コインの保有量と保有期間に応じてブロックの生成成功確率が設定され、報酬は金利相当が与えられる。コインを多く持っている参加者が成功確率が高く、改ざんが可能であるが、改ざんをすると自分が持っているコインの価値の暴落を引き起こすため改ざんをするメリットがない。(64)

PoW、PoS が富める人がさらに富む仕組みであるとして、保有数と流動性の高い人がブロック生成に成功する可能性を高くする方法も存する（PoI（Proof of Importance））。NEM が採用する。(65)

リップルはバリデーターがブロック作成を行う―PoC（Proof of Consensus）。リップル自身がバリデーターとして作成していたが（承認にかかる時間は非常に短い）、第三者企業に分散する方針が取られている。Validator がトランザクション候補への同意を示した「承認申請」が送られ、各ノードは承認申請をもとに、まず 1 段階目では承認申請は UNL に登録されている Validator によりなされているか確認し、「一定時間トランザクション候補と承認申請を比較したのち、Validator の50％以上の同意を得られていたトランザクション候補の承認申請は別のノードに送信され、49％以下のものは破棄され」る。「 2 段階目でも承認申請は UNL フィルターにかけられ一定期間審査を受け」、「今度は Validator の60％以上の同意を得られていたトランザクション候補の承認申請だけが通過」する。「その後同様にして 3 段階では70％以上、 4 段階目では80％以上と段階を追うごとに必要となる同意率が上がって」いく。「こ

の作業を繰り返すことで同意率の低いトランザクション候補の承認申請が淘汰され同意率の高いトランザクション候補の承認申請だけが残り、同意率は限りなく０％か100％に近づいて」いく。(66)

また、複数のコンセンサスアルゴリズムを用いるものもある。「現時点では、Proof-of-Work, Proof-of-Stake, Proof-of-Space, Proof-of-Authority などのモノラルアルゴリズムと、より安全性が高いと考えられているハイブリッドアルゴリズムが存在する」。(67) 仮想通貨ではこのように報酬を伴うブロック作成がインセンティブとして有用であるが、管理者がチェックし、ブロックを継続する方法もある。

(4) 検証方法についての要点

チェックとして内容面のチェックと記載改ざんについてのチェックがある。内容面のチェックは機械的にチェックしうる事柄についてであり、原因関係はチェックされない。改ざんのチェックは記載の変更があったか否かについて、文書が数値化され、次ブロックが作成され、改ざんが行えない仕組みが作られる。このことを競争によって行うのか管理者が行うのかの相違が存しうる。競争的なチェックは関与者を増やしていく。管理者のチェックは管理者の利益となりうる。仲介者的チェックは単に仲介の役割を果たすにすぎない場合もある。

以上、ブロックチェーンにおいてはプログラム上の内容チェック、改ざんチェックが行われ、内容チェックについては内容の形式的チェック（計算内容も含めて）が可能であり、プログラム上どのようなチェックを行えるか考察されうる。改ざんチェックは内容の数値化による計算解が求められ、計算結果の承認が行われ、次ブロックが作成される。この手続きは報酬を伴って民主的な競争でなされる、あるいは管理者によってなされる。

共有台帳は参加者全員が台帳を共有し、不正のある場合もそのまま継続していくことになる。そしてブロックチェーンは台帳を改ざん不能にする方法であり、迅速な処理を目指し、取引安全に資するが、改ざん不能に伴う訂正不能が特色である。

四　契約法問題

１．概観

ブロックチェーンの P2P 利用が多くの場面で企図されているが、ブロックチェーンは参加者全員が書き込む共有台帳を改ざんのないことの検証を伴い、検証されたブロックは正しいものとしてチェーン状に継続していく仕組みであり、すなわち、契約に利用される場合、多数の当事者の契約が一件ずつユーザー認証（ID・パスワード）を経て秘密鍵、公開鍵を用いて共有台帳に記載され（例えば、取引所を介するビットコイン取引では、取引所のウォレットを通して取引所あるいは取引所を経由する相手

方と売買契約が記載され、それに伴うビットコインの増減が記載される。代金支払いを法定通貨で行うときは取引所を経由してインターネットバンキング、クレジットカードでなされる―取引所自体が運用益を法定通貨として準備し、交換に充てる場合もある)、ブロックごとに改ざんのないことが検証されていく。そして、この場合の個々の記載の効力の問題があり、この点、ブロックチェーンでは実際に記載するだけでなく、モバイルタイプのときはQRコードの読み取りによるシステムの働きによる共有台帳への個々の記載の効力の問題となる。そして記載の効力が問題となると共に、取引所が関わるときは取引所の落ち度がある際も問題となる。これらの問題について、意思表示等の問題として、従来のC/Sとの相違が問題となる。すなわち、C/Sの場合のサーバ作成画面に対する本人確認（ID・パスワード等）に基づく申込承諾記載（送受信が暗号化される、電子署名が用いられうる、また、クレジットカード支払いを伴う場合もある）に関する問題とP2Pの場合の共有台帳のユーザー認証を経由し、当事者間でしか読めない暗号を用いた共有台帳記載とは意思表示の効力の問題としては基本的に同様と考えられる。ただし、サーバが企業であることが多い点、サーバが巨大なプラットフォームとして活動する場合がある点で消費者問題や無効・取消の効果面の点で相違がみられる。無効・取消による記載の訂正についてはサーバが処理するか、共有台帳のために当初のプログラムの処理、ブロック全体の運営の問題となるかが異なる点であり、C/Sではサーバが企業として対応する場合が多いのに対して、P2Pの民主的運営においては訂正期待が少ない（個々の検証を経るブロックチェーン技術を用いる場合に継続していくデータの遡っての訂正が困難となる)。

このような電子的契約においては以前からなりすまし、錯誤などが問題とされ、電子消費者契約法が制定され、電子的契約に関する準則が定められている。

P2Pにおいてはこの契約が共有台帳への個別の当事者間の記載で行われ、同様の問題があり、到達時期は共有台帳記載完了時と解され、基本的に詐欺、強迫などの民法規定はP2Pにおいてもあてはまる。すなわち、例えば、詐欺、強迫によってなされた共有台帳記載は取り消しうる、錯誤による台帳記載は無効主張が可能となるのである。ただしその実効性の問題が生じる。

ブロックチェーンでは訂正方法の問題があり、トップダウン的な管理者を認めるのか、あくまでも民主的な運営をするのかで異なる。共有台帳に管理者がいる場合の訂正方法、管理者がいない場合は多数決でハードフォークを行うあるいは相手方に修正してもらうことになるが、相手方への記載の強制方法はあるのか問題となる。

強調されるのはブロックチェーン自体が、訂正を前提とせず、あくまでも前に進んでいくことを念頭に置いていく方式であるという点である。

すなわち、意思表示の欠缺・瑕疵による無効・取消は原則通り認められるのであるが、参加者が修正しないことを前提とし、欠缺・瑕疵をすべて自己責任とする制度設

計が当事者の含意により可能となるか問題となる。

サーバが管理するシステムでは、サーバの消費者法適用、自主規制などが認められる。この場合、サーバのプラットフォーム内容の恣意性の問題もある。

P2P においては管理者がいない場合に意思表示の訂正などが困難であり、当事者間での原状回復も困難である（特にグローバルな取引において）。

電子商取引において、基本的には C/S の取引を念頭に置いていたと考えられ、P2P においても同様と考えられるが、以下、個別に見る。

２．民法上の問題

(1) 成立

電子消費者契約法は、「民法の隔地者間の契約に対する例外規定」は電子承諾通知を発する場合には適用しないとする。つまり、隔地者間の契約では電子承諾通知が相手に到達したときに契約が成立することになる。民法改正は承諾の意思表示を一般に到達主義とする。

電子的契約は当事者間での電子データのやり取りで行われる。サーバ・クライアント間では、本人確認を経た電子的意思表示がサーバの様式に記載されたときに申込みの意思表示とされる（ワンクリックで契約が成立する場合もあるし、電子署名文書がやり取りされる場合もある）。（「ウェブサイトを見た購入希望者は、当該サイトの購入申込システムに従い、申込みボタンをクリックする等の方法で、契約の申込みの意思表示をする。申込みの意思表示があると、売主は電子メールなどにより承諾の意思表示をする」（到達主義）。(68)）この意思表示に民法規定の適用がある。

P2P では、契約は共有台帳記載によって行われる。この場合に双方が申込と承諾の意思表示を記載した時点、あるいはあらかじめ相手方の承諾があるとされるときは申込時点で契約が成立すると解される。

その場合にスマートコントラクトでは、一定の事実によって契約が自動的に執行される（どこまで執行できるかは契約にもよるが、代金支払いも含めて執行可能である）仕組みであり、事実発生によって自動的に合意が成立し、執行されると解されうる。

ビットコイン等仮想通貨の移動は支払あるいは購入であり、記載時に支払いあるいは所有権移転の効果が生じる。

(2) 本人確認

本人性の確認については、C/S ではサーバ（通常は事業者である）の画面において設定された ID とパスワード（ユーザー認証）によってなされる（２段階認証もなされうる）。認証された電子署名あるいはデジタル署名（秘密鍵と公開鍵を用いるもの）を用いることによって当事者の本人性を確認することができる。

ID、パスワードなど本人確認についての事前合意のある場合にはそれによって本

人に効果が帰属するとされる。その際、売主側のシステムの安全性が高く、データ漏洩のおそれが著しく低い場合にこのような事前合意は有効とされうるが、ID、パスワードによって本人側の帰責性を問わず、一律に本人に効果が帰属するという合意の場合、あるいは具体的なセキュリティシステムについての合意のないまま、本人確認の方式についての合意がなされ、セキュリティシステムの安全性が低く、データ漏洩のおそれがある場合には合意が無効とされうるとする。本人確認方法の事前合意については、売主側の提供するシステムの安全性の程度を認識しないまま合意する場合が問題となり、通常の安全性を備えない場合の合意の効力は制限されうるとする。

また、「電子署名の認証機関が十分な本人確認をせずに電子証明書を発行し、その後それが利用され、証明書を受け取った相手方がこれを信じたものの、なりすまされた本人（電子署名の名義人）への効果帰属が認められなかったために損害を受けた場合に、認証機関は証明書の受取人に対し、不法行為責任を負う」。

「反対に、電子署名の名義人への効果帰属が認められた場合には、認証機関は、そのことにより損害を受けた当該名義人に対し、原則として不法行為責任を負う」。(69)

認証機関がホームページにおいて認証業務規定を公開し第三者が証明書を受け取る際にそれを承認する旨応答する場合、この規定に反する事柄については債務不履行責任も存しうる。この場合には規定における免責条項の有効性も問題となる。(70)

データが改ざんされないこととともに、データ作成者の本人性が保障されなければならない。

P2P 型ネットワークでもユーザー認証が必要となり、「認証サーバを設置したり、公開鍵基盤（PKI）を利用して認証が行われているが、どちらの方法でも、サーバや認証局（CA）を設置、運用する必要がある。」そのため、認証情報を分散ハッシュテーブルを利用してネットワーク内で分散、保持するワンタイムパスワード等が提案されている。(71)

データのやり取りにおいて作成者（送り手）と受け手の本人性保障についてはデジタル署名（当事者でしか作成・復号できないことの保障）という方法（送信者が秘密鍵で暗号化したデータを受信者が公開鍵を用いて復号する。この方法でも受信者に代わってデータを改ざんした者は暗号化できない（秘密鍵がわからない）。ただしデータ自体はサーバが管理する）が利用されているが、ブロックチェーンはデータをサーバが管理せず、ブロック作成ごとにそれ以前のブロックのすべてのデータの検証が行われる点で、信頼度がより高い（個々のブロックの書き込みには秘密鍵、公開鍵が用いられる―受け手が秘密鍵と公開鍵を作り、公開鍵を送り手に送り、送り手が公開鍵で暗号化したデータを受け手が秘密鍵で複号する。このデータの改ざんのないことが検証される）。

ビットコインでは、ウォレットに収納された秘密鍵と公開鍵のキーペアリストを用

いて取引がなされる。

秘密鍵はビットコインアドレスに結び付いたビットコインの所有を示す（秘密鍵を他者に与えることは処分権を与えることを意味する）。所有者は秘密鍵を用いて暗号化したビットコインを相手方のビットコインアドレスに送り、相手方は公開鍵を用いて復号する。その後自己の秘密鍵を用いて暗号化して送ることになる。(72)

(3) ハッキング

ハッキングにより、なりすましての財産窃取などが行われうる。

ハッキング行為自体が刑事罰を受ける。不正アクセス禁止法は、不正アクセス行為、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止し、刑事罰を定める。

また、それによって財産的な損害を受けた場合、不法行為による損害賠償請求が可能である（加害者が特定できれば）。

不正アクセス行為による本人名義の取引についてはなりすましの問題となる。

(4) なりすまし

本人ではないものが本人として行為するいわゆるなりすましは本人に効果が帰属しないが、取引安全の保護から表見法理に基づいて効果が帰属することがあり得る。準則によると本人確認についての事前合意のない場合には原則として効果が帰属せず、a) 外観の存在、b) 相手方の善意無過失、c) 本人の帰責事由により表見代理規定の類推適用が生じうるとする。

なりすましについて、「電子商取引の一回的取引においては、原則として冒用者の行為の効果は本人に帰属しないが、表見代理の類推適用の結果」、「本人に効果が帰属する可能性がある」。「継続的な電子商取引やクレジットカード利用について」、「前者の場合、本人確認合意が原則として有効であり、通常はIDとパスワードの使用があれば本人に効果が帰属することになる」（消費者契約では本人確認合意が無効となる場合がある）。内容の暗号化も利用される。より慎重には認証された電子署名を用いる（暗号鍵作成者の本人確認の証明（電子証明書）を経た共通鍵暗号方式・公開鍵暗号方式の利用）。

「クレジットカードの不正利用についても（基本的には本人がカード番号、名前、有効期限、キーを記入する）、本人確認合意の有効性が問題となるが、クレジットカードについては、不正利用に関する利用規約の内容が特殊かつ詳細であり、カード名義人（本人）に不利なものではないことから、消費者契約法の適用により無効となることは少ないと思われる」。インターネットバンキングにおける不正払戻しには民法478条の適用がある（銀行の免責条項については判例上過失のない場合のみ適用があるために同様となる）。(73)

なりすましは本人の帰責事由による場合とセキュリティに問題がある場合とある。

P2P においても、本人を冒用しての意思表示は原則として効力がない。

無断で本人確認を使用したものについても同様であるが、表見代理の適用があり、本人確認措置のハッキング・流出についての過失の有無が問題となる。またなりすまされた法律行為の効力に関して、約定の効力、免責条項の効力が問題となる。

P2P において支払いにクレジットカード、インターネットバンキングを利用することができ（例えば、仮想通貨で取引所が関わる場合）、その場合の不正利用はカードの不正利用などと同様の問題となる。支払いに仮想通貨が用いられる場合はブロック記載の問題である。

(5) 未成年者

未成年者の年齢確認を経た後の意思表示について、詐術にあたるか否かは、「年齢、商品・役務の対象の性質、事業者の宣伝・勧誘方法、年齢・同意確認のための事業者の設定する画面表示や構成、その他親権者の同意なしに未成年者が取引することを困難にするための仕組み」など個別に判断される。(74)

P2P 共有台帳記載においても同様であり、未成年者の意思表示は取り消しうるために年齢確認措置が必要となる。また、P2P 利用についての詐術の有無も総合的に判断されうる。ただし、個別記載の訂正が困難なため、取消の効果の実効性はない。

(6) 錯誤

錯誤について、民法理論に基づき無効主張が認められる（事業者・消費者間では消費者契約法、電子消費者契約法）。

価格誤表示では多くの場合、誤表示が申込みの誘因であり、申込後、承諾の到達により契約が成立すると考えられるために、その段階で錯誤の成否となる（表意者には重過失があると考えられるために、相手方が誤表示と認識していたかどうかが問題となる）。(75)

P2P 共有台帳記載においても同様である（無効の効果の実効性はない）。

(7) 詐欺、強迫、公序良俗違反

相手方に欺罔行為、強迫行為がある場合、内容面で公序良俗に反する合意については、民法理論に従って取り消される、無効主張が認められる。P2P 共有台帳記載においても同様である。

(8) 意思表示一般

P2P 共有台帳においても意思表示論一般に通常と同様の無効・取消が認められうるのであるが、管理者自身の権限の問題もあり、説明義務が緩められる問題、P2P の民主制から取引安全システムの事前同意の効力、免責条項の効力などが問題となる。P2P 共有台帳運営について、民主的に運営される場合は原則として自己責任となる。台帳運営者が管理者の場合はシステム運営責任があり、仲介者の場合は仲介者としての責任となる。

(9) 所有権移転

台帳記載によって物の所有権が移転するが、ビットコインの所有権が移転するか問題となる。ビットコインの所有権について東京地判平成27年８月５日 LLI は、「所有権の対象となるか否かについては、有体性及び排他的支配可能性が認められるか否かにより判断すべきである」とした上で移転に他者の関与が必要であり、ビットコインの保有量を示さない仕組みであることから、保有者の排他的支配がないとしてビットコインの所有権を否定する。「ビットコインネットワークの参加者は、ビットコインの送付先を指定するための識別情報となるビットコインアドレスを作成することができ、同アドレスの識別情報はデジタル署名の公開鍵（検証鍵）をもとに生成され、これとペアになる秘密鍵（署名鍵）が存在する。秘密鍵は、当該アドレスを作成した参加者が管理・把握するものであり、他に開示されない」。「一定数のビットコインをあるビットコインアドレス（口座Ａ）から他のビットコインアドレス（口座Ｂ）に送付するという結果を生じさせるには、ビットコインネットワークにおいて、①送付元の口座Ａの秘密鍵を管理・把握する参加者が、口座Ａから口座Ｂに一定数のビットコインを振り替えるという記録（トランザクション）を上記秘密鍵を利用して作成する、②送付元の口座Ａの秘密鍵を管理・把握する参加者が、作成したトランザクションを他のネットワーク参加者（オンラインになっている参加者から無作為に選択され、送付先の口座の秘密鍵を管理・把握する参加者に限られない。）に送信する、③トランザクションを受信した参加者が、当該トランザクションについて、送付元となる口座Ａの秘密鍵によって作成されたものであるか否か及び送付させるビットコインの数値が送付元である口座Ａに関しブロックチェーンに記録された全てのトランザクションに基づいて差引計算した数値を下回ることを検証する、④検証により上記各点が確認されれば、検証した参加者は、当該トランザクションを他の参加者に対しインターネットを通じて転送し、この転送が繰り返されることにより、当該トランザクションがビットコインネットワークにより広く拡散される、⑤拡散されたトランザクションがマイニングの対象となり、マイニングされることによってブロックチェーンに記録されること、が必要である。このように、口座Ａから口座Ｂへのビットコインの送付は、口座Ａから口座Ｂに『送付されるビットコインを表象する電磁的記録』の送付により行われるのではなく、その実現には、送付の当事者以外の関与が必要である」。「特定の参加者が作成し、管理するビットコインアドレスにおけるビットコインの有高（残量）は、ブロックチェーン上に記録されている同アドレスと関係するビットコインの全取引を差引計算した結果算出される数量であり、当該ビットコインアドレスに、有高に相当するビットコイン自体を表象する電磁的記録は存在しない」。「上記のようなビットコインの仕組み、それに基づく特定のビットコインアドレスを作成し、その秘密鍵を管理する者が当該アドレスにおいてビットコインの残量を有しているこ

との意味に照らせば、ビットコインアドレスの秘密鍵の管理者が、当該アドレスにおいて当該残量のビットコインを排他的に支配しているとは認められない」。(76)

残量は明記されないが計算上明らかであり、他者の関与も直接当事者間の取引には関係せず、むしろ当事者の不正をチェックしうる性質のものであるので、ビットコインの所有権を考えることは可能である。ビットコインはむしろ通貨としての問題、金融商品としての問題が主たる問題である。

その後、同様に MTGOX 社関連の事案であり、取引所利用者の破産債権についての破産裁判所の査定に対する異議審の東京地判平成30年１月31日金判1539号８頁は、流失したコインについてのコイン債権を認めず、アカウント情報のあるデータベースに記録されたビットコイン等の残高について届出破産債権を認める。

３．消費者保護問題

事業者・消費者間の取引においては消費者保護規定が問題となる（消費者契約法、電子消費者契約法）。特定商取引法は危険な販売方法について規制するものであり、通信販売はその規制する販売方法のひとつであり、販売促進がもたらされる（特に信用販売と合わさって販売促進がもたらされてきた）。

C/S ではサーバが事業者であることが多い。

P2P で共有台帳記載当事者が事業者・消費者間である場合は消費者法が適用されるが、適用方法が問題であると共に個別記載の訂正は原則としてできない。

(1) 消費者契約法

消費者契約法は詐欺、錯誤、強迫などに関して事業者・消費者間の契約について民法を修正する。このように当事者の属性による契約法規定が存し、P2P におけるブロックでの事業者・消費者間の記載、仲介者を介したその記載、管理者との取引記載等に適用されうる。

(2) 電子消費者契約法

電子的意思表示は到達主義が取られ（改正法は全般に到達主義をとる）、C/S ではサーバのボックスに記録された時点とされる。

電子消費者契約とは、消費者と事業者との間で、「電磁的方法により」、「電子計算機の映像面」を介して締結される契約であって、画面に従って消費者が電子計算機を用いて申し込み又は承諾の意思表示をするものである。

「民法の錯誤の例外規定」は、消費者が行う電子消費者契約の申込み又はその承諾の意思表示について、その契約の要素に錯誤があった場合であって、当該錯誤が次のいずれかに該当する場合は適用しない。

消費者が電子消費者契約の申込み又はその承諾をする意思がなかったとき。

消費者が電子消費者契約の申込み又はその承諾の意思表示と異なる意思表示をする

意思があったとき。

但し、事業者側が意思表示の確認処置を講じた場合又は消費者からそのような確認処置が不要であるという意思の表明があった場合は、この限りではない。

消費者の意思表示が事業者の画面の指示に従って行われる場合に消費者の錯誤無効の主張に対して、事業者は重過失を主張できない（確認措置を講じていない限り）。

申込みの最終段階（最終確認画面）において、申込内容を表示し、訂正手段を提供し、決定ボタンに注文決定であることが表示されていることが要求され、行政処分の対象となる。

P2P でも同様であり、錯誤無効は主張されうるが、実効性はない（行政処分が課されるか問題となる）。

(3) 特定商取引法

顧客の意に反して契約の申し込みをさせようとする行為(77)

「①あるボタンをクリックすれば、それが有料の申込みとなることを消費者が容易に認識できるように表示していないこと」、「②申込みをする際に、消費者が申込みの内容を容易に確認し、かつ、訂正できるように措置していないこと」。

また、特定商取引法14条顧客の意に反して契約の申込をさせようとする行為を禁止し、経産省によって「インターネット通販における『意に反して契約の申込をさせようとする行為』に係るガイドライン」が公表されている。

P2P においてどのような手段を用いてこのような表示がなされうるか問題であるが、インターネット特有の問題としては、安易に契約がなされうると共に代金の支払いが迅速に行われてしまうという点がある。確認措置と併せて、契約手続のしくみについての何らかのチェックが必要となる。そもそもお互いの意思表示の適正さが重要な問題であり、インターネットにおいてはその点で不十分となるおそれがある。適正な意思表示を求めていく方法と適正でない場合の危険をどのように負担するのかが考察されなければならない。

(4) 割賦販売法

事業者・消費者間の分割払いによる（信用販売を利用する）契約に割賦販売法が適用され、インターネット取引にもあてはまり、無効・取消、行政処分が課される。インターネット取引の支払い手段としてのクレジットカード決済において契約の無効・取消の際の金銭の返還については相手方の自主的返還があれば直ちに行われうるが、それがない場合は支払いを止めることができる場合は限られ、支払われたものの返還については裁判を起こすなど手続的には困難を伴うものであった（近時の割賦販売法改正）。

インターネットバンキングなどインターネットでの金銭の誤移動については誤振込の考え方が参考とされ、返還困難であると考えられる。また、この場合にブロック

チェーンを用いる P2P 取引での仮想通貨での支払いも同様と考えられるのであるが、ここでも修正方法が問題となる（後述）。

(5) 消費者問題概観

消費者契約法、特定商取引法、割賦販売法などは事業者・消費者間の契約について適用され、電子的契約においても同様である。

C/S の契約ではサーバが事業者であることが多く、相手方であるとき、これらの特別法の適用を受ける。ただし、オークションなどサーバが単に個人間の仲介の役割を果たすにすぎないときは適用されないとされる（仲介契約には適用される）。P2P におけるブロックチェーン記載による契約においても、事業者・消費者間のやり取りはこれらの特別法が適用されると解される、すなわち、ブロック内の事業者・消費者間の取引記載に当てはまると解され、無効・取消の効力は発生すると解されるが、ブロックの当該個別記載を修正することはできない。P2P では台帳運営者自体は当事者ではなく、参加者全員あるいは管理者・仲介者である。管理者の場合はシステム運営責任であり、仲介者の場合は仲介者としての責任である。P2P で台帳が民主的に運営される場合は原則として自己責任となる。

消費者を主体とする問題については P2P において相手方が事業者か否かの判断、その際に事業者である場合に個々に効果を変えなければならないこと、また仲介取引において P2P 共有台帳取引一般に消費者法の適用を認めるのかも問題となりうる。

ここでも P2P が消費者問題を回避し、自己責任を前提とする制度設計を可能にするのかが問題となる。

4．電子決済

電子決済とは、従来はクレジットカード、インターネットバンキングなどによる法定通貨の移転の問題であり、原因関係との関係が問題となる（誤振込判決や近時の割賦販売法改正）。電子マネーは法定通貨のハードタイプでのデジタル化であり、原因関係は影響しないと解される（それ自体を無効化できず、当事者間の不当利得返還の問題となる）。仮想通貨による支払いはブロック記載であり、原因関係は出てこないが、原因関係が影響するのかという問題は提起しうる。

従来の電子決済についても契約一般の問題、なりすましの問題がある。即ちこのようなシステムを用いることの伝統的契約理論による説明の問題、システム特有の理論の問題がある。さらに、電子決済については誤った口座間の移動をどの範囲で修正できるのかという問題もある。例えば自己の口座の金銭を間違った口座に振り込む場合、自己の口座の金銭を他人が使用する場合などである。

「クレジットカード決済においては、カード番号、有効期限の記載、セキュリティコード、本人情報によって決済がなされる。無断で自らのカード番号、有効期限が使

用された場合、会員規約においては、表見代理となる場合、会員規約上の義務違反により帰責事由のある場合を除いて本人は責任を負わないとされる。現行実務上、カード会員はカード、番号について善管注意義務を負い、義務違反のない場合には支払い義務を負わない（加盟店から情報が漏洩した場合には責任を負わない)。義務違反のある場合には支払い義務を負うが、本人に故意または重過失のある場合（他人に貸与した場合)、家族や同居人などカード会員の関係者が使用した場合など本人の責任が大きい場合を除いて、カード会社の負担、あるいはカード会員規約に含まれる保険によって補填されるとする。また、第三者のカード情報の不正使用についてはカード会社が支払い請求しない扱いをする場合もある。」

インターネットバンキングにおいては、パソコン等を通して、口座開設、投資信託取引、振込、残高照会、入出金の確認などが24時間できる。インターネットバンキング決済においては、約款において、本人確認の方法について事前合意がなされ、その方法が用いられていればなりすました者による資金移動も有効とされる。このような約款の効力については銀行のセキュリティシステムの安全性も考慮される。東京高判平成29年３月２日金判1525号26頁は、不正送金に対する銀行の事前・事後の諸義務を否定する。

「コンピュータを通した契約に関して上で見てきたように、全体としてインターネット取引がスムーズに行われることが優先的に考慮される。即ち、電子的な方法による意思表示の効力、本人確認が定められた方式に則って行われる場合には有効なものとして確定することになる。合意された方式の適正さの問題、システムの安全性の問題も考慮されなければならないのであるが、この点については銀行の資金移動に関する判例が参考とされる。そして、コンピュータを通してクレジットカード番号、キャッシュカード番号が盗用された場合、支払いミスが行われた場合の処理については通常の場合の処理が参考とされる。

最判平成５年７月19日判時1489号111頁は、『銀行の設置した現金自動支払機を利用して預金者以外の者が預金の払戻しを受けたとしても、銀行が預金者に交付していた真正なキャッシュカードが使用され、正しい暗証番号が入力されていた場合には、銀行による暗証番号の管理が不十分であったなど特段の事情がない限り、銀行は、現金自動支払機によりキャッシュカードと暗証番号を確認して預金の払戻しをした場合には責任を負わない旨の免責約款により免責されるものと解するのが相当である』とするが、基本的には同様の議論が当てはまる。ただし、最近においては本人確認が厳しくなっており、盗難通帳については厳しい扱いのものも見られる（盗難通帳について暗証番号を確認すべきとする)。また、最判平成15年４月８日判時1801号28頁は盗難通帳と暗証番号による払戻しについて、銀行の通帳機械払いシステム管理責任において無権限者による払戻を排除するための注意義務としての通帳機械払いの払戻につい

て明記すべき義務を尽くしていないために478条の保護を受けないとする。

誤振込については最高裁判決のように、有効な預金債権が成立する可能性があるが、コンピュータを通した振込についても基本的には同様の議論が当てはまる。

誤振込においても、キャッシュカード、クレジットカードの盗用においても、判例に反対する見解もあり、慎重な取り扱いもなされているのであるが、判例の立場に立ち、さらにインターネット取引において取引安全を重視しようとする傾向からすれば、元に戻す処理ではなく、そのままの取引状況を継続する処理がなされる可能性もある。このことはシステム特有の理論が優先しうることを意味しうる（金銭の物権的な性質よりも定められた手続に基づく預金債権の成立など契約的処理が優先されうる）。ただし、コンピュータを通したカード番号の盗用、手続ミスの問題については、セキュリティの問題と共に管理者責任の問題も生じる。即ち、充分なセキュリティが講じられていない場合の盗用に対しては盗用された者だけの責任ではないとすること、充分な回復措置の講じられていない手続ミスに対してはミスした者だけの責任ではないとすることが考えられ得る。この場合に、システムを管理する者にも安全性、ミスの是正措置などの責任が存しうる。即ち、銀行の資金移動に関する判例でも述べられていることであるが、主体的な運営をなす者の責任も考慮されなければならない。また、手続、本人確認を厳密にし、セキュリティの安全性を高めることは可能であるが、完全なセキュリティを望むことができず、厳密な手続のためにかえって危険性が高くなる恐れもあるために、管理責任が重要と考えられる。この点において追及などの金銭所有権自体の物権的効力を強く認めることが重要となってくるのである」。(78)

電子マネーとは、「通貨によって先払いされた金銭価値（単位）をデータ化したりして、決済の段階で金銭単位のデータをやり取りし、このやり取りされた金銭単位に応じて、予め先払いされ蓄えられた通貨」と相殺するものであり、紙幣・硬貨使用のわずらわしさからの解放、決済の迅速化・確実性の向上を目指し、「さらに、プリペイドカードやキャッシュカードと連携、携帯機器を利用したシステムの運用によって、家計を一元管理することも可能と」し、「ネットでの支払い手段としても使用でき」、「認証手段の導入により、紛失時の経済的損失の防止も可能」とする。

決済にはオンライン方式、オフライン方式があり、「オンライン方式の場合は直接クレジットカード会社または電子マネーのサービス会社のホストコンピュータと、小売店等の決済用端末をオンラインで接続し決済を行」い、クレジットカード等と類似する。オフライン方式は、「金銭価値を電子化（情報機器や記憶媒体に置き換えること）して磁気カードやICカードなどに収納し、小売店等の決済端末によりオフライン決済を行う」。

「利用のための実体としては非接触型決済のICカード（IC搭載の携帯機器等を含

む）や、その他のプリペイドカード類が必要であ」り、端末（カードリーダ）との間で暗号化された読み出し、書き込みを行う。

「紛失・盗難や、不正使用（横領、詐欺など）が起きた場合には、電子マネーの価値の逸失のほか様々な経済的損失が生じる可能性があり」、「この点は、貨幣経済における貨幣・紙幣についても紛失・盗難などによる価値の逸失があるのと同様で」ある。

「ただし、電子マネーに関しては情報技術によりその IC カード類や利用アカウント（利用権）に対して名義を登録する事が可能な場合があり、その場合には、電子マネーの提供事業者によっては、紛失・盗難時に本人確認を伴う届け出により、利用停止措置、電子マネーの再発行を受け付ける場合がある」とされる。(79)

P2P 契約における代金の支払いがクレジットカードで行われる場合、クライアント・サーバ契約と同様に契約の無効・取消は直接的にはクレジットカード支払いに影響しない。ただし、クレジットカードの取り扱いの問題となり、即時の撤回、異議申し立てが認められる場合はある。P2P での仮想通貨の支払いはブロック記載であり、原因関係とは無関係と解される。また、P2P を利用した仮想通貨の移転それ自体の無効・取消も問題となる。

5．契約問題（意思表示と無効・取消）

ここで問題となるのが P2P の民主的運営方法の問題と記載の大量性に伴う個人情報問題と共にブロックチェーンの確実性（実質的に改ざんできない大量のデータが共有される）に伴う契約法問題である。ブロックチェーン技術の特色はデータが継続し、追跡可能であること（記載は暗号で行われる）、ブロック記載の訂正ができないことであり（相手方の訂正するための反対取引記載による）、P2P の特色は当初のシステム（アルゴリズム）に基づき運営され、その後は民主的に改善され、管理者なしに機能しうることである。例えば、ビットコインでは通貨としての利用を可能にするシステムにより本人確認後、取得・移転の暗号記載（トランザクション）と共に手数料を差し引いて残高処理される。これらの記載されたブロックについては PoW により検証継続していき、システムあるいは内容に問題があると考える場合はハードフォークあるいはソフトフォークを行い、分岐が行われうる。その他の仮想通貨においても基本的に同様であるが、システムの利用方法を多様に認めることができ、承認方法も多様に認めることができ、運用権限を管理者に認めることもできる（P2P では民主制が特色となるが、中央のノードを用いる集中型を利用することもできる(80)）。どのような管理を行うか、その方法は有用となりうるか問題となる。仮想通貨以外の P2P 利用において、例えば民泊事業においては管理者（仲介者）が重視されている。あくまでも民主的処理を重視しようとする場合には自己責任原則が強調される。

そして、これらの立場の相違は法的には当事者の意思表示の効力が問題となり（改

ざん・なりすまし、意思表示の欠缺・瑕疵、消費者保護、物権的効力)、意思表示原則通りに無効・取消が認められるのであるが、当事者の地位の相違に基づく法律効果（例えば消費者保護）をどう考えるのか、無効・取消が認められる場合の記載の是正方法、物権設定・移転記載の効力が問題となる。無効・取消などの効果を台帳記載ではなく、当事者間での返還で行うことはもちろん可能である（実際には強制困難である)。台帳記載は訂正できない（ハードフォークは可能であるが)。ブロック全体を承認しないことによる訂正も考えられるが、承認については迅速性が要求される。このように台帳訂正についてはシステムとして事前に規制するのか、ハードフォークとして事後に行うのかの問題もある。そして、その際には当初のシステムの問題があると共にそれぞれ訂正の煩雑さが問題となり、そもそも取引安全を念頭に置くブロックチェーンシステムとの整合性が問題となる（事前規制を慎重にすると時間的な問題があり、事後訂正を重視すると民主制の問題がある)。

五　意思表示の無効・取消の訂正方法と管理者（前提と運用、事前と事後）

１．意思表示の訂正方法

意思表示としてのブロックチェーンへの記載の法的効力については通常の意思表示理論による無効・取消が認められるが、ブロックチェーンは台帳の改ざんのないことを検証していくために、記載を訂正することができない（意思表示が無効である、取り消された場合でも記載を正せない、物権の設定・移転を否定できない、仮想通貨による支払いを否定できない、相手方から逆方向の記載を行うことはできるが、強制できない。相手方に対する不当利得返還請求は可能であるが、実効性がない)。記載を訂正する方法として当該記載の含まれるブロックとは別の新たなブロックを発生させるハードフォーク（仕様の変更などで用いられる）があるが、それを行う方法が困難である（全員が新しいものに移行する、あるいは分岐した両方が安定すれば問題はない)。プログラムによる内容チェック、プルーフオブワーク（PoW）などの承認方法において承認を行わないことも考えられるが、こちらも実行方法が困難である（迅速性に問題が生じる)。また、事前チェックは形式的なものであり、事後チェックは当該取引を無効にするのではなく、ブロックに記載された取引全体を無効にする点でも問題が生じる。

このようにブロックチェーンは記載の訂正が困難であるために、P2P の下で自己責任による大きな取引保護を認めるものである。したがって、管理方法が問題となる。承認制度をどのように行うのか、ハードフォークをどのように行うのかである。いずれも当該ブロックチェーンの当初のシステム（例えば仮想通貨のアプリケーション）がまず問題となる。当初プログラムに記載された承認、ハードフォークが記載された

方法に従ってなされる（当初プログラムが全員一致によるとするのか、多数決によるとするのか（ビットコインは過半数による－フルノード・SPV ノードで検証方法が異なる(81)－51%問題)、権限を持つ者が行えるとするのか、任意の者が自己のものについて行えるとするのか)。当該ブロックチェーンに参加する者は当初のプログラムに従うことを前提に参加する。そして、ハッキング（なりすまし）などによる記載の無効の実効性のために承認を行わない、ハードフォークを行うなどが当初のプログラムに従って行われる。しかし、実際には当初のプログラムはそこまで記載せず、創設者・管理者など知識を有する者によって行われる場合がある。

したがってまず問題となるのが、当初のプログラムの内容承認の方法、ハードフォーク実施方法とその方法に対する参加者の承認である（前提問題)。前提問題としての当初プログラムの拘束力である。プログラムに対する参加者の認識とプログラムに従う合意はどのような場合（プログラムにおけるブロック運営に関する情報提供とそれについての参加者の同意）に成立し、プログラムの拘束力がどの問題について認められるのか、その際に実質的に運営権を持つ者は参加者の承認を根拠とできるかである。

次に当初プログラムに記載されていない事項、修正すべき事項をどのように行うかである（内容問題－前提問題と内容問題は概念的には明確に区別されるが、実際上の区別は困難であり、プログラムに対する参加者の同意が厳密になされない場合が多いと考えられる)。承認規制によって事前に規制するのか、ハードフォークによって事後的に規制するのか、民主的に修正するのか、管理者が修正するのかなど当初プログラムと異なるが、なすべきと考えられる事柄をどのように実施していくのかである。ブロック管理を民主的に行うのか、管理者が権限を持って行うのかである（自由か管理か)。自由は恣意となるが、民主的管理がうまく機能すれば発展する。ただし、民主制自体を過大評価してはならない。管理は後見的保護を与えうるが、依存を生み出し、支配を正当化する問題がある（現在の巨大プラットフォームの評価も必要となる)。基本的には個人の権利を強く認める必要があり、管理者に依存することなく、記載の訂正を認める方法が検討されるべきであると考える。

これらの問題について、基本的にはどのような管理システムが取られるのかが重要となり（民主制を重視するのか、管理者の地位を重視するのか)、そこでまた、内容承認方法を規制するのか、ハードフォークを規制するのか問題となり、自己責任を原則とするのかか、管理者に何等かの責任を認めるのか問題となり、その際に創設者の利益と共に、P2P の発展性をどう考えるのか、多様な利用をどう考えるのかが関わり、それでも管理者権限を強くすべきであるのか、その場合の従来のプラットホーム企業との関係などが考察されなければならない（仮想通貨の場合、取引所は個人のウォレットの創設を保持する、売買を行う、売買の相手を見つけるなど個人の取引を補助

するものであり、顧客とは委任契約を行うものであるが（顧客の仮想通貨を預かる）、ブロックチェーンの管理については自ら仮想通貨所有者としてかかわるに過ぎない）。管理者の態様に応じて管理者の責任を重くすべきか、P2P の発展性のために自己責任を貫くのか、後見的役割を持つ者を用いるのかである（パブリックブロックチェーンとプライベートブロックチェーン）。基本的な立場としては個人の権利を強く認める方法が考察されるべきである（一定の場合に個人によって訂正できる方法が認められるべきであるとともに慎重な民主制をとるべきである―迅速性、取引安全に問題が生じても）。

２．仮想通貨創設者（システム管理者）

仮想通貨創設者はプラットフォーム作成者としてあるいはその後の仮想通貨管理者としての権限を有しうる。

例えば仮想通貨創設者は自らプログラムして仮想通貨を作成することができ、オープンソースプログラムを利用して作成することができ、他の仮想通貨をハードフォークさせて作成することができ、他の仮想通貨をそのシステムに基づく新たに作成したものと交換することができる。これらのことから、仮想通貨の管理方法としては個人が主体となるものと考えられるが、有用な仮想通貨となるためにはできるだけ多数のネットワーク利用が必要となり、管理を巨大なプラットフォーム企業に委ねた方がよいとも考えられる。

仮想通貨創設者（管理者）は作成プログラムに基づき不正記載に対して事前に形式的チェックを行い、事後にハードフォークを行うことができる。

ビットコインでは創設者は管理を民主的な方法に委ね。すべての参加者が競争的に報酬を伴ってブロック作成することを可能とし、すべての参加者が承認を行うとした。それによって民主的な運営がなされたが、ブロック作成に時間がかかると共に多数者による分岐が可能であり、多数者による不正の可能性があった。

ブロック作成・承認方法としては創設者が行う、一定の管理者に委ねるなどの方法も可能であった（PoS, PoI など）。

以前見たように、創設者は事前の内容チェックのためのプログラムをどのようなものにするか決定することができる。参加者はプログラム内容を承認して参加するが、プログラムの修正などについて管理者が権限を有する場合があり、また参加者の多数が修正することも可能であり、分岐も可能である。

また、管理者はハードフォークを実施することができる（多数者も可能である）。

ハードフォークとは「ブロックチェーンの永続的な分岐（分裂）を引き起こす仕様変更のこと」であり、コインの分裂のため（参加者の対立）、アップデートのため（新ブロックのみ作用する）、アルトコイン生成のために行われる。

「アップデートのためのハードフォークとは、ブロックチェーンの課題や、プロトコル（中枢の仕組み）を改善するため」（セキュリティの向上や、トランザクション（取引データ）処理能力向上など）「に参加者の賛同を得て実行される仕様変更」とされる。

イーサリアムでは「Proof of Work から Proof of Stake への移行」。「取引データをまとめたブロックのブロックチェーンへの追加のしやすさを、『計算処理能力→コインの保有量』に変更する」ハードフォークが2017年11月になされた。(82)

「イーサリアム上で構築された Tha Dao というサービスの脆弱性を突かれて約50億円分のイーサリアムがハッカーに盗まれた事件」への対応としてハードフォークが行われた。「ハッキング自体をなかったことにするため、ブロックチェーンをハッキング前の状態のものに戻す施策が、多くの有識者の支持を得て実行」された。ただし、その措置に反対する者はイーサリアムクラシックとして元のブロックを継続する。(83)

ブロックチェーンをハッキング被害前の状態に戻すという、ハードフォークを伴う仕様変更案に対して、「ソフトフォークによって、既存のルールを変更することで資金を回収しようとする試みが検討され」たが、「『Dos 攻撃に対する脆弱性が発見されたこと』や『資金の回収に時間がかかること』などの懸念点があったため、結局ソフトフォークは実行されず、ハードフォークが実行され」た。

「プロトコル以外の問題に関して対応策を講じるというのは、『非中央集権的なイーサリアムプラットフォームの理念に反する』」とされる。(84)

このように P2P においてもできる限り多人数のネットワーク形成が有用となるが、巨大なプラットフォームが管理するものも考えることができる。

P2P は広範な民主的ネットワークを可能にするものであり、ブロックチェーンは文書の確実性をもたらすシステムであり、両者を通して新たなネットワークの創設が企図されるのであるが、ブロックチェーン文書の確定性は過度の取引安全をもたらすものであり、そのネットワークが問題に対応するのか、新たな管理者（プラットフォーム）を置くことができるか、それによって、恣意的管理者の問題、新たなプラットフォーム問題が生じるのか考察されなければならない。民主的システムにおける管理問題、取引安全に偏したネットワークのプラットフォーム問題である（従来、例えば Amazon のような取引を統括するサーバとしてのプラットフォームには情報独占による市場独占の問題が存するとされる）。

取り戻すための制度として管理者が正当に介入できる制度が要請されうる。通常の金融においては金融緩和の要請、金融機関の独占的地位など同様の問題を有するものであったが、金融機関の受託者的地位が役立つ（受益者の物的保護）。ブロックチェーン・分散型台帳技術利用の共通問題としての意思表示論と物的権利論、無効・取消とその効果、誤決済とその効果、改ざんとその効果などの問題について受託者的地位の考察が役立つ。

また、仮想通貨の場合、マネー・ローンダリングとの関係では以下の点が参考となる。

「リスクベース・アプローチとは、金融機関等が、自らのマネロン・テロ資金供与リスクを特定・評価し、これを実効的に低減するため、当該リスクに見合った対策を講ずることをいう。マネロン・テロ資金供与の手法や態様は、その背景となる犯罪等の動向のほか、広く産業や雇用の環境、人口動態、法制度や、IT 技術の発達に伴う取引形態の拡大、経済・金融サービス等のグローバル化の進展等、様々な経済・社会環境の中で常に変化している。手法や態様の変化に応じ、マネロン・テロ資金供与対策は、不断に高度化を図っていく必要がある。近年では、情報伝達の容易性や即時性の高まり等により、高度化に後れをとる金融機関等が瞬時に標的とされてマネロン・テロ資金供与に利用されるリスクも高まっている。金融機関等においては、マネロン・テロ資金供与リスクを自ら適切に特定・評価し、これに見合った態勢の構築・整備等を優先順位付けしつつ機動的に行っていくため、リスクベース・アプローチによる実効的な対応が求められる」。

「主なものは以下のとおり。特定事業者による疑わしい取引の届出の要否の判断は、当該取引に係る取引時確認の結果、当該取引の態様その他の事情のほか、犯罪収益移転危険度調査書の内容を勘案して行わなければならない（犯収法第８条第２項）。犯罪収益移転危険度調査書の内容を勘案して犯罪による収益の移転の危険性の程度が高いと認められる取引については、疑わしい取引の届出の要否の判断に際して統括管理者による確認等の厳格な手続を行わなければならない（犯収法第８条第２項、同法施行規則第27条第３号）。特定事業者は、犯罪収益移転危険度調査書の内容を勘案し、以下の措置を講ずるように努めなければならない（犯収法第11条第４号、同法施行規則第32条第１項）」。①自らが行う取引について調査・分析した上で、その結果を記載した書面等を作成し、必要に応じて見直し、必要な変更を行うこと。②特定事業者作成書面等の内容を勘案し、必要な情報を収集・分析すること、並びに保存している確認記録及び取引記録等を継続的に精査すること。③高リスク取引を行う際には、統括管理者が承認を行い、また、情報の収集・分析を行った結果を記載した書面等を作成し、確認記録又は取引記録等と共に保存すること。④必要な能力を有する従業員を採用するために必要な措置を講ずること。⑤必要な監査を実施すること。(85) このようなことは、ブロックチェーンの民主的運営では行うことができず、管理者の権限強化が必要となる。また実際、違法に移転した金銭等を元に戻す方法が検討されなければならない。

３．仮想通貨取引所・販売所

「取引所とは取引の場を提供するプラットフォームで、ビットコイン等の仮想通貨ウォレットを持ったユーザー同士がビットコインの売買を行う場所」であり、「取引

はユーザー同士の相対取引で行われ、取引所は売買取引に関与せずに手数料を徴収する方式が一般的で、売り主・買い主双方が取引相手の属性情報の交換なしで取引ができる環境の提供場所が取引所となっている」。

「販売所は運営主体が取引相手になり、販売所提示価格での仮想通貨等の売買を行う。ただし、販売所提示価格は購入提示価格が最新の取引価格より高く、買い取り提示価格は安く設定することが通例で、この差額『取引所スプレッド』が販売所の収益となる」。

取引は所有者の持つ秘密鍵と送金先のアドレス（公開鍵）で行われるが、取引所で管理が行われる場合、秘密鍵も取引所が管理する。

「現在ビットコイン等仮想通貨取引を行う大半の投資家は、秘密鍵の管理を取引所に委託した形で口座を保有しており、コイン所有者が自らの秘密鍵を知らないケースが殆どであるので、「取引所の信頼性・セキュリティの堅固さ」が重要となっている」。

「取引所でビットコイン等を購入した場合には、秘密鍵に関する情報を得ることはできない。購入したビットコイン等は、取引所の管理するウォレット（デジタル通貨の金庫・財布に相当する）に入り、秘密保護の観点からもユーザーがその情報を知ることはできない」。

「取引所が所有している秘密鍵がハッキングされると、マウントゴックスの破綻時の様に不正アクセスにより数百億円相当のビットコイン盗難という事態が発生する。

「取引所のセキュリティ確保方法は各種あり、コールドウォレットや、マルチシグネチャウォレット（一つのアドレスに複数の秘密鍵を割り当てる）等が多くの取引所で導入されている」。(86) この点、取引所のハッキングによる個人被害がみられた。

取引所は個人と仲介的な役割のために個人に対して責任を負うことがあるが、ブロックチェーンに対しては通常の参加者としての立場があるに過ぎない。

個人との適切な関係のために取引所の組織などの安全性が確認されなければならず、金融庁は登録制度を実施し、監査を行う。資金決済法は、商品券やプリペイドカードなどの金券（電子マネーを含む）と、銀行業以外による資金移動業について規定し、仮想通貨も対象とする。

現在、仮想通貨交換業を営むには金融庁の登録が必要となる。(87)

登録審査は、「まず事務ガイドライン（チェックリスト）による形式検証、いわば書類選考から始められる。続いて専門官による現場ヒアリングが必要に応じて実施され、システム管理体制、マネー・ローンダリング・テロ資金供与対策、利用者保護に向けた取組みを確認、さらに当該の会社役員や株主、関係会社、監査法人等にリスクが無いかなど、実質面重視の審査」がなされる。(88)

2018年６月７日 FSHO 株式会社に出された登録拒否処分は以下のように述べる。(89)

金融庁が平成30年２月19日以降、立入検査を実施したところ、犯罪による収益の移

転防止に関する法律に基づく取引時確認を行っていないほか、疑わしい取引の届出の要否に係る判断を行っていない事例等が認められた。同年３月８日、１か月の業務停止命令及び業務改善命令（これまでの取引に関する取引時確認の実施及び疑わしい取引の届出の実行、マネー・ローンダリング及びテロ資金供与対策態勢の構築等）を発出した。

その後、金融庁は改善状況を確認するため、同月23日以降、２回目の立入検査を実施したところ、依然として、マネー・ローンダリング及びテロ資金供与対策にかかる業務の改善が図られていない状況が判明し、平成30年４月６日、２か月の業務停止命令及び業務改善命令（経営体制の抜本的な刷新、法令等遵守や適正な業務運営を確保するための実効性ある経営管理態勢の構築等）を発出した。

平成30年５月16日以降、３回目の立入検査を実施したところ、下記のとおり、管理態勢の整備に問題があることが認められた。

経営管理態勢については平成30年５月６日付株主総会及び取締役会において、代表取締役社長、取締役及び監査役を選任するなどの措置を実施したとしているが、経営上極めて重要な案件について、旧経営陣が、新代表取締役社長の承諾を得ることなく進めるなど、依然として旧経営陣が実質的に当社を支配している実態が認められ、同年６月４日、旧経営陣である株主により臨時株主総会が開催され、同年５月６日付株主総会の役員選任決議を無効とする旨の決議がなされている。このように、当社においては、経営体制が何ら刷新・構築されていないほか、内部監査を実施する体制を整備していないなど、４月６日付業務改善命令を履行していない状況にあり、経営管理態勢は未だ整備されていないものと認められる。

法令等遵守態勢については取引時確認を実施すべき特定取引を行った者のうちの半数以上の者について、依然として取引時確認を完了させていないほか、多数の疑わしい取引が確認され、ようやく当該取引に係る届出が行われる事態が生じている。また、取引時確認を行った確認記録が作成されていない多数の事例（犯収法第６条違反）等が確認された。さらに、株主・役職員について、反社会的勢力であるか否かの確認を一切行っていないほか、顧客に対しての確認も不十分なものとなっている。

法定帳簿等管理態勢については、検査実施日である平成30年５月16日までに、法定要件を満たした帳簿の作成を完了していない。また、法定帳簿の元となる取引記録データのうち、取引日、売買価格、手数料の各項目に関し、申込書記載事項との相違が複数認められ、正確性が確保されていない。

システムリスク管理態勢については未だにシステムリスクの特定・分析・評価を網羅的に実施しておらず、また、コンティンジェンシープランも作成していない。

利用者保護等管理態勢については、取り扱う仮想通貨の概要や、利用者が支払うべき手数料等を顧客への説明書面に記載していないなどの法令違反（法第63条の10、仮

想通貨交換業者に関する内閣府令第17条第１項違反）が認められるなど、利用者保護等管理態勢は未だ整備されていないものと認められる。

この点について、金融機関のフィデュシャリー・デューティーが取引所についても言われる。フィデュシャリー・デューティーとして仲介者の信認義務と共に顧客財産の物権的保護が問題となりうる。このことは取引安全の要請とも調和する。このように当事者の物的権利の強化が要請される。

４．シェアリングエコノミーのプラットフォーム企業

シェアリングエコノミーにおいてブロックチェーンが用いられる場合、仲介者としてのプラットフォーム企業が管理する。

Airbnb は、宿泊スペースを持つ登録ホストとそれを必要とするゲストの間を直接つなげるプラットフォームを運用する会社であり、自ら在庫を持つことなく宿泊事業を営むものであり、マッチングによる手数料を収益とする。(90)

Airbnb 利用規約(91)によると、予約変更、キャンセルは直接プラットフォーム上、あるいはカスタマーサポートで行うことができ、返金方法も定められている。ホストのキャンセルに対する制裁について Airbnb は裁量を持つ。(92) ホスト・ゲスト間の紛争について、ゲストが宿泊施設又は宿泊施設に存在する私物等に損害を与えた旨を証拠を提示して請求する場合、問題解決センターを通じて支払いを求めることができると共に Airbnb に損害請求の裁定を求めることができ、ゲストに責任があると判断した場合、Airbnb Payments は、支払規約に基づき、損害請求を償うのに必要なすべての金額をお客様又は本保証金（適用ある場合）から徴収するとされる（保険請求も可能)。(93) ゲストは Airbnb プラットフォームの利用に適用されるすべての法令、規制及び税務上の義務を遵守する。

Airbnb の事前の書面による承認を得ずに、使用目的以外の目的（第三者のサービス、アプリケーション又はウェブサイトへ参加させるためにメンバーを募集又はその他の方法で勧誘することを含みますが、これらに限られません）で他のメンバーと連絡を取ることは禁止される。サービス料の支払いを回避するため、又はその他何らかの理由により、Airbnb プラットフォームとは無関係に予約をリクエストし、予約し若しくは予約を承認することを目的に、Airbnb プラットフォームを利用することも禁止される。(94) 現状での利用状況について免責条項がある。(95)

民泊事業においては、以上のように、ホスト・ゲスト間の紛争解決が重要な問題となり、あらかじめ解決金、解決方法が定められており、仲介者に強い権限が認められている。ブロックチェーン記載の無効・取消等の場合の当事者間の解決に仲介者がどのように関わるのか問題となる。

わが国では住宅宿泊事業法（民泊新法）によって宿泊事業者に厳しい規制が課され

るとともに仲介者に登録制度が実施される。

Airbnb はもともとはサーバとしてホストとゲストを結び付けていたが、現在はブロックチェーンを利用する。ブロックチェーンにおいて仮想通貨での支払いを可能とすると共に信頼できるデータの共有化も可能とする。そして、ブロックチェーンにおいても仲介者としての Airbnb 自体の役割は変わらず、Airbnb がブロックチェーンを管理すると考えられる。(96) ここでもフィデュシャリー・デューティーを考察することができる。

5．準則における管理者（運営事業者）の責任

このようにブロックチェーンにおける契約について、ビットコインでは当初プログラムに基づき民主的な運営が行われるが、プログラム作成者が管理を行う場合もあり、管理者の役割が重要であるとも考えられる。「電子商取引及び情報財取引等に関する準則」改訂案（平成30年 5 月21日）は以下のように述べる。

インターネットにおけるユーザー間取引に関するサービス運営事業者の責任について、(1) サービス運営事業者が取引に実質的に関与しない場合　①原則としてサービス運営事業者はユーザーに対して責任を負わない（サービス運営事業者が、単に個人間の取引仲介システムを提供するだけであり、個々の取引に実質的に関与しない場合は、ユーザー間の取引によって生じた損害について、サービス運営事業者は原則として責任を負わない)。 ②例外として、例えば、インターネット・オークションにおける出品物について、警察本部長等から競りの中止の命令を受けたにもかかわらず、オークション事業者が当該出品物に係る競りを中止しなかったため、落札者が盗品等を購入し、盗品等の所有者から返還請求を受けた場合などについて、損害賠償義務を負う可能性があるとされる。(2) サービス運営事業者が取引に実質的に関与する場合　サービス運営事業者が、自らが提供するシステムを利用したユーザー間取引に、単なる仲介システムの提供を越えて実質的に関与する場合は、その役割に応じて責任を負う可能性がある。(97)

(1) について、以下のように説明される。「インターネット・オークション、フリマサービスなど、ユーザー間の取引の場を提供するには様々な類型があり、それぞれの類型、サービスごとにユーザー間の個々の取引へのサービス運営事業者の関与の程度が異なる。一般論としては、サービス運営事業者の個々の取引への実質的関与の度合いが高いほど、ユーザー間取引に関するトラブルにつきサービス運営事業者が責任を負う可能性が高くなるといえる」。「また、サービス運営事業者は、利用規約において利用当事者間の取引の成立や内容に関して一切関与しない旨定めていることが多いが、利用規約による責任制限はどのように機能するのであろうか。利用当事者間の取引に関するトラブル以外にも、例えばシステムの維持・管理等に関するサービス運営

事業者の責任等も問題となりうる」。(98)

サービス運営事業者と利用者との法的関係は、原則として利用規約に従う。「例えば、インターネット・オークションにおいては、ユーザーとしてオンライン登録する際に、利用規約への同意クリックをすることでサービス運営事業者とユーザーの契約となる（利用規約の効力に関しては、本準則I-2-1「ウェブサイトの利用規約の契約への組入れと有効性」を参照）」。「かかる利用規約には、サービス運営事業者が責任を負う場合、負わない場合が明記されていることが多い。ただし、ユーザーが消費者の場合、消費者契約法の適用がある」（免責条項の制限）。(99)

「サービス運営事業者が、単に個人間の売買仲介システムを提供するだけであり、個々の取引に実質的に関与しない場合の事業者の責任　前記のとおり、ユーザー間取引プラットフォームには様々な類型がある。このうち、サービス運営事業者は単に個人間の売買等の取引仲介のシステムのみを提供し個々の取引に実質的に関与しない形態のサービスにおいては、一般論としては、取引は各ユーザーの自己責任で行われ、サービス運営事業者は責任を負わないと解される。すなわち、サービス運営事業者はシステムを提供する形で取引の仲介をする役割を果たすが、実際の取引行為の当事者となるわけではない。このような場合、一般にサービス運営事業者は、単に取引の場やシステムの提供者にすぎず、個別の取引の成立に実質的に関与するわけではない。したがって原則としてユーザー間の取引に起因するトラブルにつき責任を負わないものと解される（利用規約においても、ユーザー間の売買契約に関してサービス運営事業者は一切関与せず、したがって責任を負わない旨規定していることが多い）。ただし、サービス運営事業者はユーザー間の取引行為にかかる情報が仲介されるインフラシステムを提供していることから、一定の場合にはサービス運営事業者に責任を認める余地がある。すなわち、サービス運営事業者は、取引の『場』を提供している以上、法律上の性質論としてはいろいろありうるが、いずれにせよ一定の注意義務を認めることが可能と考える。例えば、インターネット・オークションにおいて、出品物について、警察本部長等から競りの中止の命令を受けた（古物営業法第21条の７参照）にもかかわらず、オークション事業者が当該出品物に係る競りを中止しなかったため、落札者が盗品等を購入し、盗品等の所有者から返還請求を受けた場合などにおいて、当該オークション事業者は、当該落札者等に対して、注意義務違反による損害賠償義務を負う可能性があると解される。」(100)

(2)「実際のサービスでは、サービス運営事業者は、様々な場面で単なるシステム提供者を越えた役割を果たしている場合もある。このような場合のサービス運営事業者の責任は、役割に応じて個別具体的に検討する必要がある」。サービス運営事業者がユーザーの出品行為を積極的に手伝い、これに伴う出品手数料又は落札報酬を出品者から受領する場合、例えばインターネット・オークションやフリマサービスにおけ

るブランド品の出品等に関し、オークション事業者がユーザーから電話で申込みを受け、当該ブランド品をサービス運営オークション事業者宛てに送付してもらい、サービス運営オークション事業者がユーザー名で出品行為を代行し、出品に伴う手数料や落札に伴う報酬を受領する場合には、サービス運営オークション事業者は出品代行者であり、単なる場の提供者ではない。サービス運営オークション事業者は、出品物を手にして偽ブランド品かどうか確認できる立場にあり、その上で出品者の出品行為を代行したのであるから、利用規約の規定如何にかかわらずトラブルの際、買主に対して責任を負う可能性がある。このような場合、依頼を受けて出品代行する商品が古物営業法上の「古物」に該当する場合には、サービス運営オークション事業者は同法の規制を受ける可能性がある。(101) 特定の売主を何らかの形で推奨する場合、サービス運営事業者が、特定のユーザーを推奨したり、特定のユーザーの販売行為を促進したり、特定の出品物を推奨した場合には、その推奨・促進の態様如何によっては、サービス運営事業者はユーザー間の取引に起因するトラブルにつき責任を負う可能性がある。例えば、単に一定の料金を徴収してウェブサイト内で宣伝することを越えて、特定の売主の特集ページを設け、インタビューを掲載するなどして積極的に紹介し、その売主の出品物のうち、特定の出品物を「掘り出し物」とか「激安推奨品」等としてフィーチャーするような場合には、売買トラブルが発生した際、サービス運営事業者も責任を負う可能性がないとは限らない。(102) サービス運営事業者自体が売主等の取引等自社となる場合、イベント性ある特別なユーザー間取引プラットフォームなどにおいて、第三者が供出した出品物につき、サービス運営事業者自体がシステム上は売主等の取引当事者として表示されているが、実際の売上金（計算）は直ちに出品物提供者に帰属する場合がありうる。このような場合には、サービス運営事業者は原則として売主等の取引当事者としての責任を負う。(103)

（3）システムの維持・管理等に関する責任等、ユーザー間のトラブル以外の問題に関するサービス運営事業者の責任。プラットフォームにおいては、手数料を徴収するものが多いが、有料、無料にかかわらず、サービス運営事業者とユーザーとの間には、サービス運営事業者が提供する取引仲介システムを利用することに関して契約関係が成立しているものと解される。例えば、インターネット・オークションやフリマサービスの場合、事業者の提供するシステムを利用しない限り、ユーザーは出品や入札・購入等の利用行為ができないからである。したがって、サービス運営事業者は、個人間の情報交換のインフラである自らが提供するサービスにかかるシステムの機能を維持・管理する義務を負うものと解される。(104)

６．検討

準則によると取引に関与しない運営事業者と関与する運営事業者で責任の有無が区別される。関与する場合とは積極的にかかわる、推奨する、あるいは自社が売主となる場合とされる。またそれとは別にシステムの維持に関する責任がありうるとする。

準則に言う運営事業者の責任とシステム作成者の責任（ブロックチェーン創設者（管理者）の責任）は異なり、ここで重要なのはシステム作成者の責任である。

ブロックチェーンは改ざんできない仕組みが取られ、取引安全が尊重されるのであるが、ハッキングによるなりすまし被害などの不正行為に対してどのような対応を採るべきか問題となる。

ブロックチェーン創設者はプログラム作成者として民主的運営がなされる場合には関与者の同意があるものとして原則として責任を負わないと考えられる。民主的運営においては前提に対する関与者の同意から関与者の運営問題となる。恣意的プログラムに対して管理者の責任が生じると共に、管理者として一定の権限を保持する場合はプログラムの改善を行う、ブロック管理する等の責任が生じうる。

いずれも取引所などの仲介者については別の問題となる。わが国では仮想通貨交換業者の規制があるだけである。

仮想通貨でのブロックチェーン利用では確実性、迅速性が重視され、民主的運営よりも管理者運営が優れていると思われるが、管理者への責任追及体制の確保が必要となる。仲介者が仮想通貨を利用する場合、仲介者はブロックチェーン管理を行うと共に、当事者の紛争の解決に寄与する方法を持たなければならない。

ただし、ブロックチェーン自体取引安全を志向するものであり、関与者もそれを前提とすると考えられる。

ブロック創設者の当初システムの内容と参加者の同意、その修正方法、ハードフェーク実行方法と参加者の関与方法、全体として多数決で行うか、管理者に権限があるのか、以上についての参加者の同意が検討されなければならず、どのような組織がとられているかが重要な問題となる（悪用に対して組織はどのように対応しているのか）。

また、管理者の問題を考える上で、巨大プラットフォームの検討、比較が必要となる。

六　プラットフォーム問題

１．プラットフォーム企業

モノ、サービスの情報を集約したプラットフォームは消費者とプロデューサーを結びつける。

「プラットフォームは取引を円滑化することによって、価値を創造する。直線的な

ビジネスが、商品やサービスを作ることで価値を生み出すのに対して、プラットフォームはつながりを作り、取引を『製造する』ことで価値を生み出す」。プラットフォームのコア機能は、1. オーディエンス構築、2. マッチメーキング、3. 中核的ツールとサービスの提供、4. ルールと基準の設定であり、それによってネットワークを構築・維持し、そのつながりを取引に変える。交換型とメーカー型があり、「消費者とプロデューサーの直接取引を最適化することで価値を提供するプラットフォームと、プロデューサーが補完商品を作り、それを大規模なオーディエンスに向けて公開または頒布できるようにすることで価値を生み出すプラットフォーム」がある（マッチング意思が異なる）。交換型には、1. サービスマーケットプレース、2. プロダクトマーケットプレース、3. 決済プラットフォーム、4. 投資プラットフォーム、5. ソーシャルネットワーキングプラットフォーム、6. コミュニケーションプラットフォーム、7. ソーシャルゲームプラットフォームがあり、メーカー型には、1. コンテンツプラットフォーム、2. 開発プラットフォームがある。それぞれコモディティ化のレベルの高いものから低いものがある（自動マッチングか検索機能重視か）。(105)

インターネットの発展と共にプラットフォームが重視されてきた。プラットフォームとは「商品やサービス・情報を集めた『場』を提供することで利用客を増やし、市場での優位性を確立するビジネスモデル」(106) であり、コンピュータの様々な機能を統合する、また、多くのサーバを統合するシステム・サーバであり、windows, apple, google, amazon などの広範なプラットフォームだけでなく（大きなプラットフォームはクラウドサービスを提供している―クラウドサービスは利用者の依存を増大させる）、フィンテックなど個別分野のプラットフォームも重視される。フィンテックはクラウドコンピューティング、モバイルプラットフォーム、マシンラーニングを利用した資産運用、融資、決済と IT を融合させる技術サービスの提供であり、金融の拡大に役立つものである（金融とプラットホームの関係は大きな問題となる）。

従来の「供給サイドが主導する経済においては、企業は経営資源をコントロールし、徹底的に効率化を押し進め、五つの競争要因（新規参入者の脅威、代替品や代替サービスの脅威、買い手の交渉力、売り手の交渉力、競争の激しさ）がもたらす難題を跳ね除けることによって、市場で強大な地位を築く」。「これとは逆に、インターネット経済の原動力は需要サイドの規模の経済、すなわちネットワーク効果である。ネットワーク効果は、ソーシャルネットワーキング、需要の集約、アプリケーション開発など、ネットワークの拡大に寄与する現象を効率化する技術の力によって、高まっていく。インターネット経済において競争相手よりも「量」を稼ぐ企業、つまり、より多くのプラットフォーム参加者を獲得する企業は、トランザクション当たりの提供価値も併記すると高くなる。」「大規模なネットワークはより大きな価値を創出し、それがより多くの参加者を引き寄せるために、さらに価値が増大する」(107)（Microsoft の抱

き合わせ販売事例のようにプラットフォームが何らかの行為を強制する場合は独禁法の問題となるが、個々の事業者は関係することを暗に強制される）。

電子商取引において独占的地位を有する者について、データと競争政策に関する検討会の基本方針は「データの集積・利活用それ自体は、競争を促進し、イノベーションを生み出す。一方で、データの集積によって、独占や寡占（競争の制限）をもたらしうる企業結合や、市場における地位を利用した消費者・中小企業からの不当な収集（搾取）、あるいは不当な「囲い込み」に対しては、独占禁止法による対応が必要。個人データのポータビリティの促進とともに、産業データのオーナーシップに関する議論や、国や法定独占産業等のデータの利活用推進に向けた議論の深化が望ましい」とする。(108)

サーバを基軸とするネットワークからP2Pを基軸とするネットワークが拡大し、シェアリングエコノミーといわれる新たな経済発展がもたらされうるとともに新たなプラットフォーム戦略が必要とされていく。ブロックチェーンなど分散型台帳技術は現在のプラットフォーム内のP2P相互関係の形成に便宜をもたらすとともに、P2Pとして現在のプラットフォーム外の新たな個々の集団形成とそれに伴う取引の発展をもたらす（新たなプラットフォーム）。またそれはビットコインに表されるように新たな金融にも便宜をもたらす（プラットフォーム内外において）。このようにブロックチェーン技術に基づくP2Pネットワークの新たな可能性は現在のプラットフォーム独占に新たな競争をもたらすものであり、サーバに依存しない参加者の自主性に基づくものでありうるが、不正是正手段など管理の方法が問題となる（ブロック管理者を置くのかどうか、どのように管理するのか、管理者にどのような権限を認めるか、ブロックに関わる者を集約するサーバに管理権限を認めるのか－仮想通貨における取引所のようにプラットフォームとしてのサーバは存する）。

２．検討

インターネットは従来、C/S（サーバのシステムにクライアントがアクセスする一対多数のネットワーク）が中心であり、改ざん（ハッキング）に対してはサーバのセキュリティが重要であった。セキュリティとして、コンピュータウィルス対策、不正侵入対策、不正コピー対策、スパムメール対策、暗号と電子認証の活用等が挙げられる。

P2Pとは複数の者の対等なネットワークシステムであり、ファイル共有が利用され、ソーシャルネットワークにとっても便宜である（サーバにおいても共有データを活用することは可能であった）。これらの組み合わせが新たなビジネスを生み出す。

C/Sにおけるプラットフォーム支配にたいしてP2P・分散型台帳が新たな民主化をもたらすが、過大評価することはできず、新たな支配（プラットフォーム）がもた

らされうる。

インターネットによる消費経済の発展に問題はないのか。消費社会と金融拡大社会は同根であり、価値増大による経済発展の問題がある。貧富の拡大と税（社会保障）による解決である。金融に基づく経済を否定する場合は経済が停滞する。経済は停滞させるべきではないのか。

インターネットビジネスではプラットフォームが重要であるが、分散型台帳技術は新たな全員参加型ビジネスをもたらすものである。ハッキング等ブロックチェーンの悪用に対して、管理権限強化、個人の権利強化が図られなければならず、管理権限強化は行いやすいが、プラットフォームの問題がある（従来と同様のインターネットの発展）。このために管理者の依存ではなく、各自の自主性が基本となる。そして財産の取戻しが問題とされなければならない。

七　結語

このように P2P ネットワークの発展性がブロックチェーン技術によってもたらされうるためにブロックチェーン技術によるデータ記載の効力がその発展性との関係において問題とされうる（今までの電子商取引における電子文書の意義と同様の問題であるが、実質的な意味は異なる。記載に対するサーバの対応とセキュリティの問題から共有データの記載の効力と管理方法の問題となる）。

ブロックチェーン技術はビジネスを変革する。P2P の発展は民主制をもたらすのか、現在のプラットフォーム独占の改善か新たな独占か。

ビットコインは金融の増大をもたらす。基本的にはビジネスの増大、金融商品の増大は経済発展をもたらす。

このような訂正することのできないデータ連結制度において、文書記載の無効・取消、財産の取戻しなどの取引の巻き戻しはより困難であると考えられる。そもそも取引の発展において、取引安全の保護、善意者保護などの法制度が存し、電子的取引においてその維持・強化が図られてきた。今回の電子的制度の発展においてもよりその要請が強いと考えられる。しかし、ブロックチェーンの不正利用に対する是正方法が重要である。

P2P は巨大プラットフォームの独占問題に競争的に作用しうる。巨大プラットフォームは参加を強制するものと考えられるが（プラットフォームはどのような行為をするか）、P2P はそれを緩和する方向になることができ、民主的管理による新たな経済をもたらし、分散型台帳技術はそれを補助しうる（新たな独占も生み出しうる）。

１．あるべき管理

インターネット取引において自己責任を原則とする仕組みの中でのハッキングなどの不正行為の是正方法について、当初システムの拘束力をどう考えるのか（どのような参加制度か、参加の仕組みはわかりやすいのか、参加権はどのように行使するのか、適切に情報が開示されているのか等）を考慮した上で、ブロック訂正方法として事前規制が良いのか、事後訂正が良いのか考察することになる。すなわち、この問題を基本的に自己責任とするのか（利用規約で自己責任とする、あるいは民主的管理において自己責任とするなど）、あるいは不正行為の結果を事前あるいは事後に民主的に是正しうるのか（民主的運営を基礎とする場合も最低限の事務執行者は必要となる）という問題と管理者的地位にある者の問題（仮想通貨創設者を管理者とする、その他取り決めに従って一定の者を管理者とする、取引所・仲介者に管理者として一定の地位を認める、取引所・仲介者を受託者として受益権の主張を認めるなど）と共にそのような者はどのように行為すべきかという問題（約款で管理者の訂正権限を認めておくなど）とそのような者の責任問題（各人の自己責任とすべきか、管理者の責任を重く見るべきか）である（管理者のいない場合にはそもそも消費者保護が行われない）。この場合に、例えば、仮想通貨については創設者の利益取得方法－自らマイニングを行うのか、仲介手数料的なものか、自己の保有資産（創設者利益）の価値増加に限るのかなど－が問題となる。利益を得る者の管理責任を重くすべきとも考えられる。いずれもコンピュータ社会に特徴的な問題であり、ネットワーク社会の発展性と危険性の問題である。P2P、ブロックチェーンはインターネットの可能性を広げる、自主的発展が可能であり、このような発展を促進するためには利用度の増大が必要であり、そのためにも大きなプラットフォーム企業がそれを利用する、あるいは民主制を合理化するなどの方法が考察されなければならず、その下での責任問題となりうる。インターネット取引自体、取引安全に偏っているが、P2P、ブロックチェーンはさらに偏るものとなり（自己責任を原則とする）、その中での管理方法が問題となるのである（あくまでも民主的に解決するのか、管理者に適正さの担保のために一定の権限を認めるのか）。基本的には個人の権利を強く認める方法、個人によって訂正がなされる方法が検討されなければならない。

このような前提において記載の効力が問題となる。記載の効力にブロックチェーンの管理方法が関連し、ブロックチェーンの管理方法に創設者・管理者の利益が関連する。

このように、まず前提として、ブロックチェーンでのブロック記載の契約法上の効力が問題となり、P2P のシステム内容が問題となり、管理者的地位にある者を置くのか（最低限の事務的管理者は必要となる）、管理者の利益をどう考えるのか、P2P、ブロックチェーン自体の発展性をどう考えるのか等の問題がある。特に、不正行為の是

正方法として管理を強化するのか、個人の権利を強化するのかが重要な問題である。

さらに、管理者的地位にある者の問題として広大なプラットフォーム企業として強大な影響力を持つ者の問題がある（Microsoft、Apple、Amazon、Google など）。民主的運営を可能とする P2P において利用されるブロックチェーンのプラットフォームが新たな取引機会を拡大し、民主的プラットフォームとして巨大なプラットフォーム企業に代わるものとなるのか、あるいは大きなプラットフォーム企業がブロックチェーン、P2P を利用し、仮想通貨を取引に組み込むなどさらに取引機会を拡大するのかという問題である。巨大プラットフォーム企業はサーバとしての中心的役割を果たすと共にクラウドサービスを提供する。その際、例えば、Google のストレージサービスにはコンテンツ使用権の Google への付与が規定されている。(109) そして、クラウドコンピューティングサービスを提供する Amazon Web Services はブロックチェーンフレームワークを提供している。このようなプラットフォームのクラウドサービス、ブロックチェーン利用の意図と管理が問題となりうる。

プラットフォームとは共通基盤のことであるが、C/S では、サーバがプラットフォームとして大量の情報を扱い、取引を行う（マッチメイク）システムを組み立てることを意味することになり、大量の情報の集約（ビッグデータ）に伴う強大な影響力（権力）把握が問題となる（独占的地位の問題）と共にプラットフォーム自体の取引の管理方法（撤回、無効・取消などの処理方法、同様の決済問題の処理方法）が問題となる。プラットフォーム自体、単に補助的役割に徹するもの（広告料収入のみ）と取引を仲介する者（仲介手数料も取得する）がある（その他何らかの間接的な収益はあるのか）。さらにクラウドサービスは補助的役割を拡張する。また、P2P においては各人がプラットフォームとなると共に台帳を常に管理する管理者を置くこともでき、特定の管理者に権限を与えるプラットフォームの形成は可能である。従来の巨大プラットフォームが P2P におけるプラットフォームも統括するのか、従来の巨大プラットフォーム企業に対抗する新たなプラットフォームが形成されるのか、あくまでも民主的にプラットフォームが形成されるのか問題となる（若干問題は異なるが、石油、電力などにおける小規模事業者の P2P 利用がどのような発展をもたらすのかという問題と類似しうる）。そして、プラットフォームによる取引の管理方法の問題と共に支払方法の管理として銀行を通して行うこと以外に仮想通貨等の直接の当事者間の価値移転方法にハードフォーク以外の介入方法をもたらしうるのかという問題がある。さらに大きな問題として、大きなプラットフォームが取引に恣意的に関与する（莫大な情報に基づき有利な状況を形成する）場合にどのようにそれを制限、阻止するのかという問題が重要な問題となる（プラットフォームとして各人の自主性を尊重する限り問題はないが、プラットフォーム自体が過度に中間者としての利益追求の姿勢をとる場合に問題となる。フェイスブックは莫大な広告料収入を有するが、個人情

報を流出させた)。ブロックチェーンの民主的運営には各人にシステムに関する十分な情報と個人の明確な権限がなるべく多く認められなければならないために、民主的運営自体は煩雑となる（管理者を置く場合は特に個人の権利の強化が問題となる)。

巨大なプラットフォームが過度の取引安全方法としてブロックチェーンを利用し、また取引安全に偏した支払方法として仮想通貨も利用していくことになることは明白と考えられる。

以上、電子的意思表示の効力としては一般原則通りに無効・取消が認められるのであるが、無効・取消の効力としてのその是正をどのように認めるのか（承認方法、ハードフォーク)、創設者の利益に応じた管理責任を認めるのか（C/S におけるサーバのような管理責任を認めるのか)、P2P、ブロックチェーンの発展性をどう考えるのか、プラットフォームの独占的地位をどう考えるのか等がブロック記載に関する中心的問題である。どのようなビジネスをどのように民主的に運営していき、どのように補助的な管理を行うのかであり、そのために台帳記載の効力、訂正方法としてはどのようなものが望ましいのかである。基本的には個人のシステム内容の理解を前提とした個人の権利を強く認める方法、個人によって訂正がなされる方法が検討されなければならない。当事者間で個人情報をオープンにし、相手方を特定し、相手方との話し合いを可能にし、記載の訂正・物権の確保を可能にする方法が検討されなければならない。このように民主制の確保には個人の権利強化が必要とされる。

２．今後の発展と問題点の解決方法

仮想通貨の問題は異なる二つの問題からなる。一つは、P2P とブロックチェーンの発展性と利用管理についての法的問題、すなわちシステムにおける意思表示の効力の問題（当初システムの拘束力の根拠と範囲、事前規制と事後規制、民主的管理と後見的管理の問題)、もう一つは。金融拡大の経済的意義の下での規制外の私的金融（金融機関によらない金融）の意義とその金融商品としての問題（仮想通貨取引の問題）である。

コンピーターは大量のデータを蓄積し、多数の人を瞬時につなげ、多くの便宜を図るものであり、この利用の促進を今までは C/S において、基本的なシステムを定め、処理するサーバが媒介者として中心的役割を担って行ってきた。大量のデータ保持と多数の人を把握するリスク（セキュリティ、個人情報）をサーバが担ってきたのであり、それは同時にそのようなサーバが巨大なプラットフォームとして独占的地位につくことを意味した（プラットフォーム企業自体、情報の集約等の補助的な役割を重視するものであったが、自ら集約された情報を利用し、必然的に巨大化する。このことはクラウドサービスにおいてもみられる)。この大量のデータに基づく支配的構造に対して、P2P は全員がデータを持ち、需要と供給を調整し、ブロックチェーンを利

用することでセキュリティも図られるなどこれらの問題を民主的に解決することを可能にする。このシステムは発展可能性を有する（P2P の大量データ、多人数関与の民主的システムの発展性は従来の C/S ネットワークのプラットフォームを中心とする発展に対して新たな可能性をもたらす）のか（新たな支配となるのかも含めて）、旧支配的形態（公的産業支配－国家主導による資本主義、その下での巨大プラットフォーム企業による産業支配－プラットフォーム企業と公的権威の関係が依存関係となるのか、対立関係となるのか不明確である）の強大化をもたらすのかである。そして、それに伴う法的問題の一つが契約問題（無効・取消をどのように認めるのか、不正利用をどのように阻止するのか、個人は何をすることができるのか、インターネットの契約規制としては事前規制が良いのか、事後規制が良いのか）であり、もう一つが通貨・金融問題である。

まず、インターネット取引におけるプラットフォームの管理者的・保護的役割と独占的地位をどうとらえるかという問題がある。金融優位の経済社会において、インターネット社会ではプラットフォームと金融機関の関係が重要な問題となる。そして、P2P はあくまでも民主的なシステムとして自由と厳しい自己責任を前提とする民主的制度にするのか（自由と自己責任を前提とするコミュニティは可能であるのか）、後見監督的機関を持つ主導者（管理者）を備えるようにするのか問題となる。取引安全・善意者保護など後戻りさせないことが資本主義社会の発展をもたらす側面を有したのであるが（このことは金融が経済社会の中心的役割を果たすことをもたらす）、インターネット取引においてもさらに後戻りさせないことが重要と考えるのか、後戻りさせる余地・方法を残しておくべきか問題となる（サーバの役割として考察されうる）。ブロックチェーンはさらに後戻りしない社会となるために、不正利用が危惧されるものとなり、ブロックチェーンが民主的なものとならなくなるときに大きな問題が生じると共に後見監督的機能を付加すべきか問題となる。後見的機能を付加する場合は従来の強大なプラットフォームが扱うなどとなり、それに依存する構造をもたらす。このような状況で支配的な地位をめざす者の濫用をどう制限するのかの問題が生じる（コンピーターソフトウェアにおける Microsoft、Apple、多様なデータに基づく google、流通における Amazon（Amazon Web Service はクラウドサービスも行う）、個人情報に基づく facebook などはどのような問題を有するのか）。このようにブロックチェーンの取引安全とプラットフォームの後見的機能に基づく金融取引の考え方がまず問題となる。

また、金融資本の優遇、金融緩和において、金融の架空性が問題となりうるとともに民主的金融（ICO）の可能性の問題がある。全体として増えることは金融機関にとっても望ましいが、私的金融が発展することは望ましくないと考えるのであろうか、どちらも望ましくないと考えるのであろうか。金融拡大が否定され、P2P の金

融利用が否定され、仮想通貨も否定されるべきと結論されるのであろうか（結論としては両者に限定を課さなければならない）。金融緩和のイニシアティブをだれが持つべきかの問題である。

さらに、金融商品として金融商品市場において取引がなされるものであるのかも問題となる。金融商品市場は価値の変動による利益を目的とする市場であるが、損失を前提として成り立たなければならず、架空の価値の増大による損失補填を認めるべきではない（全体としての価値の増大から完全なゼロサム取引ではないが、ゼロサム取引が目指されるべきである）。この点から、仮想通貨を取り入れることによる金融商品市場の拡大は避けるべきである（架空の価値としての意義を持つデリバティブは商品として認められているが）。自由に委ねる（自己責任）場合にはまた、金融には自由の危険性が大きい、金融にはそもそも自由が認められない、価値自体が限定的である、デリバティブ的な架空の価値増加が否定されるべきであると考えるのか等である。

こうして金融の拡大は正しいのか、金融拡大は金融機関が行うべきか、民間が行ってもよいのか、金融拡大としての金融商品の拡大（デリバティブ等）は是正されるべきであるのか、金融さえあれば事業活動が可能となる状況は制限すべきかという問題が仮想通貨の金融としての中心的問題である（システムの問題を伴う）。

取引が重視される社会、取引安全を法的に重視する対応は金融の優位をもたらす。事業活動が利益となる可能性が高く、事業に対する融資が利益となる。事業者が融資を得ることが成功の可能性を高める。全体として事業が利益となる可能性が高いと考えるのが取引社会である。このことは金融の優位をもたらす。そして、今日、ブロックチェーンは取引安全に基づくものであり、仮想通貨は新たな金融である。これらの問題を取引発展を重視する社会の下で、取引に対する利害関係者、特に金融機関の問題とみるか、取引社会自体の批判的考察が必要と考えるかである。資本主義社会とは、交換社会が金銭を媒介とすることによって、金銭が独自の価値を有するようになり、金銭の形での利益が交換社会の主たる目的となり、金銭を有する者がさらに利益を獲得していく構造を持つ社会である。必然的に金融機関が多大な権力を持つ社会である。そして、この社会は架空の価値による価値の増大をもたらすことにより、より価値の偏在する社会となっていく。多くの価値に伴い全体としての利益が増えるのであるが、大きな富を有する者はより大きな富を有することとなり、一部を還元する。この金融増加による自転車操業的社会が是正されなければならない。このことは価値の架空性の排除によってもたらされる。現物の裏付けのある金融商品と差額決済商品であるデリバティブ・先物の相違、同様に保険商品と架空保険商品の相違、仮想通貨と架空通貨の相違が問題とされなければならない。経済の発展とは金融が増え続けることではない。今後、仮想通貨の金融問題を続稿において取り扱っていく。

注

＊本論文作成にあたり、広島市立大学情報科学研究科教授石田賢治先生に貴重な御助言を頂きました。厚く御礼申し上げます。

（1）https://ja.wikipedia.org/wiki/Web_2.0

（2）http://gaiax-blockchain.com/byzantine-generals-problem

（3）架空性について、拙稿「循環取引の法的諸問題」法政研究17巻１号１頁、「デリバティブ取引の法的諸問題について」同18巻１・２号１頁。

（4）https://nandemo77.com/2017/10/20/make2ndbtc/

（5）https://bittimes.net/news/14129.html

（6）個々の利用方法の詳細は、赤羽喜治・愛敬真生『ブロックチェーン　仕組みと理論』（2016）41-68頁。

（7）赤羽喜治・愛敬真生『ブロックチェーン　仕組みと理論』（2016）34頁。

（8）日本経済新聞社編『仮想通貨バブル』（2018）14頁以下。

（9）https://moblock.jp/articles/17289

（10）https://www.nic.ad.jp/ja/basics/terms/p2p.html

（11）アンドレアス・M・アントノプロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳『コンサイス版ビットコインとブロックチェーン』（2018）27頁。

（12）https://www.nic.ad.jp/ja/basics/terms/p2p.html

（13）アンドレアス・M・アントノプロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書27頁。

（14）https://ja.wikipedia.org/wiki/Peer_to_Peer

（15）岩田真一『P2P がわかる本』（2005年）102-3頁。

（16）岩田真一前掲書113-4頁。

（17）https://www.nic.ad.jp/ja/basics/terms/p2p.html

（18）file:///F:/ 電子商取引及び情報財取引等に関する準則・情報の掲示利用.pdf「電子商取引及び情報財取引等に関する準則Ⅱインターネット上の情報の掲示・利用等に関する論点」

（19）file:///F:/ 電子商取引及び情報財取引等に関する準則・情報の掲示利用 .pdf

（20）https://ja.wikipedia.org/wiki/Peer_to_Peer

（21）ブロックチェーンビジネス研究会『60分でわかる！ブロックチェーン最前線』など多くの文献で指摘されている。

（22）北野宏明「ブロックチェーンの活路は人工知能との連携にあり」ハーバード・ビジネス・レビュー 2017年８月29頁。

（23）Daniel Drescher 著、株式会社クイープ訳『徹底理解ブロックチェーン』（2018）297頁。

（24）株式会社ブロックチェーンハブ著増田一之監修『実践ブロックチェーン・ビジネス』（2018）138頁以下。ブロックチェーンの広範な利用方法について、本書が詳しい。

（25）北野宏明「ブロックチェーンの活路は人工知能との連携にあり」ハーバード・ビジネス・レビュー 2017年８月29頁。

（26）https://innovation.mufg.jp/detail/id=110

（27）https://innovation.mufg.jp/detail/id=232

（28）https://innovation.mufg.jp/detail/id=232

（29）https://innovation.mufg.jp/detail/id=232

（30）https://innovation.mufg.jp/detail/id=232
（31）RYUICHI TOBISAKO「SMART CNTAINERS コールドチェーンから始まる革新的ソリューション」ICO CROWD JAPAN 5 号14頁。
（32）https://innovation.mufg.jp/detail/id=230
（33）https://innovation.mufg.jp/detail/id=230
（34）https://innovation.mufg.jp/detail/id=110
（35）https://innovation.mufg.jp/detail/id=110
（36）https://innovation.mufg.jp/detail/id=110
（37）https://innovation.mufg.jp/detail/id=218
（38）日本大百科全書（ニッポニカ）の解説［矢野武］https://kotobank.jp/word/ フィンテック -1720026
（39）https://innovation.mufg.jp/detail/id=232
（40）https://innovation.mufg.jp/detail/id=110
（41）https://innovation.mufg.jp/detail/id=110
（42）https://www.enigma.co.jp/media/page-11733/
（43）Daniel Drescher 著、株式会社クイープ訳『徹底理解ブロックチェーン』（2018）291頁。
（44）Daniel Drescher 著、株式会社クイープ訳前掲書91頁。
（45）Daniel Drescher 著、株式会社クイープ訳前掲書292頁。
（46）Daniel Drescher 著、株式会社クイープ訳前掲書294頁。
（47）もともとビットコインという信用創出方法としてブロックチェーンという暗号技術が考えられたが、ブロックチェーン技術自体の利用度が高い。
（48）Daniel Drescher 著、株式会社クイープ訳前掲書295頁。
（49）中島真志「アフター・ビットコイン」32頁。
（50）https://my-ether.net/wallet-type/
（51）中島真志前掲書32頁。
（52）アンドレアス・M・アントノブロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書 6 頁。
（53）アンドレアス・M・アントノブロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書16頁以下
（54）アンドレアス・M・アントノブロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書 6 頁以下
（55）アンドレアス・M・アントノブロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書43頁。
（56）中島真志前掲書32頁。
（57）中島真志前掲書32頁。
（58）中島真志前掲書32-35頁。
（59）中島真志前掲書36-38頁。
（60）中島真志前掲書35頁。
（61）中島真志前掲書36頁。
（62）ビットバンク株式会社＆できるシリーズ編集部『できるビットコイン入門』（2017）52頁。
（63）https://japan.cnet.com/article/35119425/
（64）杉井靖典『いちばんやさしいブロックチェーンの教本』（2017）116頁、https://moblock.jp/articles/17182
（65）四條寿彦『仮想通貨リップルの衝撃』（2018）25頁。

（66）四條寿彦前掲書84頁。https://coinotaku.com/?p=8165
（67）JEV VAINSTEINS「業務における将来性のあるアルゴリズムとしての Proof-of-Activity」ICO CROWD JAPAN 4号30頁。
（68）松本恒雄編『平成28年版電子商取引及び情報取引等に関する準則と解説』97頁。
（69）松本恒雄編前掲書107頁以下。
（70）参照準則、電子署名法。http://www.c-a-c.jp/about/knowledge.html
（71）アンドレアス・M・アントノブロス著、鳩貝淳一郎編、今井崇也・鳩貝淳一郎訳前掲書16頁以下。
（72）西田雄治・辻貴介・清水明宏「P2P 型ネットワークへのワンタイムパスワード認証方式の適用」電子情報通信学会技術研究報告・信学技報105巻281号23頁。
（73）森亮二「Ⅰ－3　なりすまし」松本恒雄編前掲書22-23頁。
（74）高木篤夫「Ⅰ－4　未成年者による意思表示」松本恒雄編前掲書26頁。
（75）松本恒雄編『平成28年版電子商取引及び情報取引等に関する準則と解説』94頁以下。
（76）武内斉史「仮想通貨（ビットコイン）の法的性格」NBL 1083号10頁、末廣裕亮「仮想通貨の私法上の取扱いについて」NBL 1090号67頁、森下哲郎・増島雅和「仮想通貨を巡る法的課題」ジュリ1504号 2 頁、片岡義広「仮想通貨の規制法と法的課題（上）（下）」NBL 1076号53頁、1077号82頁、小林信明「仮想通貨（ビットコイン）の取引所が破産した場合の顧客の預け資産の取扱い」金法2047号40頁、藤井裕子「仮想通貨等に関する返還請求権の差押え」金法2079号 6 頁、松嶋隆弘「仮想通貨に関する法的諸問題－近時の裁判例を素材として」税理60巻14号 2 頁、鈴木尊明「ビットコインを客体とする所有権の成立が否定された事例」新・判例解説 Watch, vol 19, 59頁等がある。
（77）インターネット通販における「意に反して契約の申込みをさせようとする行為」に係るガイドライン
（78）拙稿「動産及び金銭信託受益権の物権的効力に関する解釈上の問題と電子商取引」商大論集55巻 3・4 号67頁以下。
（79）https:// お金が無い .jp/spend-money/28502/
（80）Daniel Drescher 著株式会社クイープ訳『徹底理解ブロックチェーン』（2018）26頁。
（81）https://moblock.jp/articles/17295
（82）https://moblock.jp/articles/17385
（83）https://moblock.jp/articles/17267
（84）https://moblock.jp/articles/17289
（85）https://www.fsa.go.jp/news/30/20180206/besshi1.pdf「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」 6 頁以下。
（86）https://www.money-book.jp/15542
（87）詳細については、松嶋隆弘・渡邊涼介編著『仮想通貨をめぐる法律・税務・会計』（2018）104頁以下。
（88）「FISCO 株・企業情報2018年春号仮想通貨とサイバーセキュリティ」23頁。
（89）http://kantou.mof.go.jp/rizai/pagekthp0130000001_00026.html
（90）利用規約 6.1 Airbnb プラットフォームの利用の対価として、Airbnb は、ホストに対する手数料及びゲストに対する手数料を請求することができます。6.2 適用されるサービス料は、リスティングの公開又は予約の前に、ホスト又はゲストに対して表示されます。Airbnb は、いつでもサービス料を変更することのできる権利を留保し、料金の変更が有

効となる前に、メンバーに対して料金の変更について適切な通知を行います。6.3 Airbnb にサービス料を支払う責任はお客様ご自身が負います。適用されるサービス料は Airbnb Payments によって回収されます。Airbnb プラットフォーム上に別段の定めがない限り、サービス料は返金不可となります。

(91) https://www.airbnb.jp/terms

(92) 9.1 ホスト及びゲストは、ホスト及びゲストが Airbnb プラットフォームを通じ、又は、Airbnb カスタマーサポートに指示した予約の変更について責任を負うものとし、かかる予約変更に関連する追加リスティング料金、ホストサービス料、ゲストサービス料及び税金を支払うことに同意するものとします。9.2 ゲストは、リスティングのキャンセルポリシーの規定に従い、いつでも確定した予約をキャンセルすることができ、Airbnb Payments は、総料金のうち当該キャンセルポリシーが定めるゲストの受取分を返金します。Airbnb Payments は、酌量すべき事情の存在しない限り、総料金のうち適用されるキャンセルポリシーが定めるホストの受取分を支払規約に基づきホストに送金します。9.3 ホストにより確定済みの予約がキャンセルされた場合、ゲストには当該予約の総料金の全額が、商業上合理的な期間内に返金されます。Airbnb はゲストに対し、返金額を新規予約に振り替えることを許可することができ、その場合、Airbnb Payments はゲストからの指示を待って、当該ゲストの次回の予約に当該金額を振り替えます。Airbnb はホストによりキャンセルされたリスティングについて、予約がキャンセルされた旨の自動レビューを公開することができます。また、Airbnb は、(i) リスティングのカレンダーで解約された日付を予約不可又はブロックされたままにすること、及び、(ii) ホストにキャンセル料を課すことができます。但し、Airbnb の酌量すべき事情ポリシーに基づき解約する正当な理由がある場合、又は、ゲストの振る舞いに対する正当な懸念がある場合はこの限りではありません。9.5 Airbnb は、その単独の裁量により、一定の場合に、確定した予約をキャンセルし、適切な返金及び受取金に関する決定をすることが必要であると判断することができます。この判断は、Airbnb の酌量すべき事情ポリシーに規定されている理由、又は (i) Airbnb が両当事者の正当な利益を考慮した上で、Airbnb、その他のメンバー、第三者又は財産に重大な損害がもたらされるのを防ぐために必要であると真摯に考える場合、若しくは、(ii) 本規約において規定されているその他の理由でなされる場合があります。9.6 ゲストがゲスト返金ポリシーに定めのある旅行中のトラブルに巻き込まれた場合、Airbnb は、その単独の裁量により、ゲスト返金ポリシーに従って、総料金の全部又は一部をゲストに返金することを決定することができます。9.7 ホストとして予約の代金を受け取った後、ゲストが確定した予約をキャンセルした場合、又は Airbnb が確定した予約のキャンセルが必要と判断した場合で、Airbnb がゲスト返金ポリシー、酌量すべき事情ポリシー、又はその他適用あるキャンセルポリシーの規定に従い当該ゲストに返金を行う場合には、Airbnb Payments が当該返金額を以降のお客様への受取金から控除するなどの方法により回収する権利を有することに同意するものとします。

(93) 11.2 ホストが、ゲストであるお客様が宿泊施設又は宿泊施設に存在する私物若しくはその他の財産に損害を与えた旨を証拠を提示して請求する場合（以下「損害請求」といいます)、ホストは、問題解決センターを通じてお客様からの支払いを求めることができます。ホストが Airbnb に損害請求の裁定を求めた場合、お客様は、応答する機会が与えられます。お客様がホストに対する支払いを行うことに同意する場合、又は Airbnb が、その単独の裁量により、損害請求についてお客様に責任があると判断した場合、Airbnb

Payments は、支払規約に基づき、損害請求を償うのに必要なすべての金額をお客様又は本保証金（適用ある場合）から徴収します。さらに、Airbnb は、お客様が損害請求に対し責任を負う場合において、その他の方法によりお客様から支払額を徴収し、また、この件について Airbnb に利用可能な一切の救済手段（Airbnb ホスト保証に基づきホストからなされる支払請求に関連する支払いを含みますが、これに限られません）を追求する権利を留保します。

（94）14.1（i）Airbnb の事前の書面による承認を得ずに、お客様の予約、リスティング又は他のメンバーによる Airbnb プラットフォームの利用に関する問い合わせ以外の目的（第三者のサービス、アプリケーション又はウェブサイトへ参加させるためにメンバーを募集又はその他の方法で勧誘することを含みますが、これらに限られません）で他のメンバーと連絡を取ること。・・・サービス料の支払いを回避するため、又はその他何らかの理由により、Airbnb プラットフォームとは無関係に予約をリクエストし、予約し若しくは予約を承認することを目的に、Airbnb プラットフォームを利用すること。

（95）16. 免責事項。お客様が Airbnb プラットフォーム又は総コンテンツを利用することを選択する場合、お客様は自発的に、お客様ご自身のリスク負担でこれを行うものとします。Airbnb プラットフォーム及び総コンテンツは、明示又は黙示を問わず、いかなる種類の保証も伴わず、「現状有姿」で提供されます。お客様は、お客様のリスティング又はお客様が受けているホストサービスに適用される可能性のある Airbnb サービス、法令又は規制を調査するためにお客様が必要と考えるあらゆる機会があったこと、また、Airbnb によるリスティングに関する法律又は事実の表明に依拠していないことに同意するものとします。

（96）http://thebridge.jp/2016/04/airbnb-just-acquired-a-team-of-bitcoin-and-blockchain-experts-pickupnews

（97）http://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000173994「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）

（98）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）23頁。

（99）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）24頁。

（100）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）25頁 .

（101）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）25頁。

（102）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）26頁。

（103）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）26頁。

（104）「電子商取引及び情報財取引等に関する準則」改訂案（現行版からの変更履歴付き）27頁。

（105）アレックス・モザド、ニコラス・L・ジョンソン著、藤原朝子訳『プラットフォーム革命』（2018）62頁以下。

（106）https://ferret-plus.com/6095

（107）マーシャル・W・ヴァン・アルスタイン、ジェフリーG・パーカー、サンギート・ポール・チョーダリー（有賀裕子訳）「プラットフォーム革命」ハーバード・ビジネス・レビュー41巻10号31-32頁。

（108）https://www.jftc.go.jp/houdou/pressrelease/h29/jun/170606_1.html

（109）https://wired.jp/2012/04/27/your-google-drive-files-now-in-googles-promo-materials-ars/