第１章　仮想通貨の私法上の法的性質

――ビットコインのプログラム・コードとその法的評価

加　毛　　明

１　はじめに

（１）検討の対象と理由

本稿は、ビットコインに代表される仮想通貨[(1)]の私法上の法的性質について検討する。この問題について、わが国の実務・学説では――比較法的にみても早くから[(2)]――活発な議論が展開されてきた[(3)]。その理由として、まず挙げられるのが、平成26年

(1)　金融庁・仮想通貨交換業等に関する研究会「報告書」https://www.fsa.go.jp/news/30/singi/20181221-1.pdf（2018年）31頁では、国際的な議論の動向や法定通貨との誤認防止を理由として、「仮想通貨（virtual currency）」から「暗号資産（crypto assets）」への名称変更が提案されている。しかし、本稿では、従前の議論状況を踏まえて「仮想通貨」の語を用いる。

(2)　本稿のもとになった平成28年度金融法務研究会・第１分科会報告では、仮想通貨の法的性質に関するドイツ法の議論状況についても検討を行ったが、本稿では脚注で若干の言及するにとどめる。

(3)　この問題に関する文献は枚挙にいとまがないが、代表的なものとして、以下の文献を挙げることができる。田中幸弘＝遠藤元一「分散型暗号通貨・貨幣の法的問題と倒産法上の対応・規制の法的枠組み（上）（下）――マウントゴックス社の再生手続開始申立て後の状況を踏まえて」金法1995号52頁、1996号72頁（以上2014年）、片岡義広「ビットコイン等のいわゆる仮想通貨に関する法的諸問題についての試論」金法1998号（2014年）28頁（「片岡①」）、芝章浩「ビットコインと法」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BP社・2016年）84頁（「芝①」）、片岡義広「仮想通貨の規制法と法的課題（上）」NBL 1076号53頁（2016年）（「片岡②」）、武内斉史「仮想通貨（ビットコイン）の法的性格」NBL1083号（2016年）10頁、末廣裕亮「仮想通貨――私法上の取扱いについて」ビジネス法務16巻12号（2016年）73頁（「末廣①」）、末廣裕亮「仮想通貨の私法上の取扱いについて」NBL1090号（2017年）67頁（「末廣②」）、森下哲朗「FinTech時代の金融法のあり方に関する序説的検討」黒沼悦郎＝藤田友敬編『江頭憲治郎先生古稀記念 企業法の進路』（商事法務・2017年）771頁、片岡義広「仮想通貨の私法的性質の論点」LIBRA 2017年4月号（2017年）12頁（「片岡③」）、得津晶「日本法における仮想通貨の法的諸問題――金銭・所有権・リヴァイアサン」法学81巻2号（2017年）149頁（「得津①」）、西村あさひ法律事務所編『ファイナンス法大全（下）〔全訂版〕』（商事法務・2017年）838頁〔芝章浩〕、日本銀行決済機構・金融研究所「『FinTech 勉強会』における議論の概要」https://www.boj.or.jp/announcements/release_2017/data/rel171207a.pdf（2017年）、末廣裕亮「仮想通貨の法的性質」法教449号（2018年）52頁（「末廣③」）、片岡義広

2 月の Mt. Gox 社の破綻事件である。当時の世界最大のビットコイン交換所の破綻により、日本法の倒産手続において、ビットコインがいかに取り扱われるかが重要な問題となり[(4)]、その私法上の法的性質に注目が集まることになった。さらに、平成 27 年 6 月の G7 エルマウ・サミットにおいて、マネー・ロンダリングやテロ資金供与への対策のために仮想通貨取引に対する規制の導入が求められたことを背景として、平成 28 年 6 月に、情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律が成立した。その結果、資金決済に関する法律（以下、「資金決済法」という）に仮想通貨に関する明文の規定が新設されたことも[(5)]、仮想通貨の法的性質をめぐる議論の活性化の一因と考えられる。

このようなわが国の実情に照らせば――ビットコインを念頭に置いて――仮想通貨の法的性質を検討することには、十分な理由があるように見える。実際、「仮想通貨の私法上の位置づけが不明確なままでは、それに関して具体的に生ずる問題について、私法上適用されるべき規律がはっきりせず、法的な安定性を損なうことになる[(6)]」という指摘は、Mt. Gox 社の破綻事件を通じて、日本の法律家が経験したところと重なる。

それにもかかわらず、ビットコインに代表される仮想通貨の法的性質を論じることについては、法律論に外在する事情と内在する事情の双方を理由として、その意義を慎重に検討する必要があると考えられる。

まず、外在的事情として、ビットコインの将来性には重大な疑問が提起されている[(7)]。システム上、発行量の上限（約 2100 万 BTC）が設定され、発行量が時間の経

「ブロックチェーンと仮想通貨をめぐる法律上の基本論点」久保田隆編『ブロックチェーンをめぐる実務・政策と法』（中央経済社・2018 年）156 頁（片岡④）、後藤出＝渡邉真澄「ビットコインの私法上の位置づけ（総論）（各論）」ビジネス法務 18 巻 2 号 113 頁、4 号 103 頁（以上 2018 年）、森田宏樹「仮想通貨の私法上の性質について」金法 2095 号（2018 年）14 頁、金融法委員会「仮想通貨の私法上の位置づけに関する論点整理」http://www.flb.gr.jp/jdoc/publication55-j.pdf（2018 年）、本多正樹「仮想通貨の民事法の位置付けに関する一考察（1）（2・完）」民商 154 巻 5 号（2018 年）921 頁、6 号（2019 年）1194 頁、片岡義広「再説・仮想通貨の私法上の性質――森田論文を踏まえた私見（物権法理の準用）の詳説」金法 2106 号（2019 年）8 頁（「片岡⑤」）、芝章浩「暗号資産の民事法上の取扱い」NBL1138 号（2019 年）49 頁（「芝②」）、得津晶「仮想通貨の消費者被害と法的問題」現代消費者法 42 号（2019 年）19 頁（「得津②」）。なお、末尾の【追記】も参照。

(4) Mt. Gox 社の破産手続において、ビットコインに対する取戻権の成否が争われた事件として、東京地判平成 27 年 8 月 5 日 LEX/DB25541521 が存在する。

(5) 佐藤則夫監修『逐条解説 2016 年銀行法、資金決済法等改正』（商事法務・2017 年）35 頁。

(6) 森田・前掲注（3）14 頁。

(7) 代表的なものとして、中島真志『アフター・ビットコイン』（新潮社・2017 年）53-115 頁。

過とともに漸減することから[8]、ビットコインはデフレーションの傾向を備える[9]。このことを背景として、現実のビットコインの取引においては――開発者が想定していた決済手段としての利用ではなく――投資（投機）目的での取引が大半を占めている。その結果、法定通貨に換算したビットコインの価格は極めて変動が大きいものとなっている。このような事情からすれば、今後も、ビットコインについて、決済手段としての利用が拡大するとはいい難いように思われる。

さらに――決済手段としての利用に限らず――ビットコインの取引自体の将来性についても、懐疑的な見方が存在する。後述のように、ビットコインの取引を支える仕組みとして重要なのが、ビットコイン・トランザクションを集積したブロックを検証する作業（マイニング）である。現在までのところ、マイニングを行うインセンティヴは、報酬としてビットコインを付与すること（コイン・ベース報酬）によって確保されている。しかし、システム上、マイニングの報酬とされるビットコインの発行量は21万ブロックごと（期間にすれば約4年ごと）に半減するものとされているため[10]、今後、マイニングを行う者が減少し、ビットコイン・システムを維持できなくなる可能性が指摘されている。この懸念は、マイニング・プールと呼ばれる集団によるマイニングの寡占状況のもとで[11]、より深刻な問題となる。

それゆえ、現在の金融実務の関心は、ビットコインに代表される仮想通貨というより、むしろ、その前提とするブロックチェーン技術の多様な利用可能性に向けられているということができる。従前のわが国における仮想通貨の法的性質に対する関心が、ビットコイン取引の実務的重要性を前提としていたのだとすれば、ビットコインの将来性に対する消極的評価は、仮想通貨の法的性質を論じることの意義に疑義を投げかけることになる。

次に、法律論に内在する事情として、仮想通貨の法的性質に関する議論が、個別の法律問題の解決に直結しないという問題がある。例えば、仮想通貨の帰属・移転について多様な法律構成が主張されているにもかかわらず、「仮想通貨の帰属・移転の規律に関する総論レベルでの議論が各論レベルでの帰結の違いをもたらすとは限らな

(8) アンドレアス・M・アントノプロス（今井崇也＝鳩貝淳一郎訳）『ビットコインとブロックチェーン――暗号通貨を支える技術』（NTT出版・2016年）〔Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media 2014〕184-185頁。

(9) アントノプロス・前掲注（8）186-187頁。

(10) アントノプロス・前掲注（8）183-184頁。

(11) マイニングの寡占状態の形成については、アーヴィンド・ナラヤナンほか（長尾高弘訳）『仮想通貨の教科書――ビットコインなどの仮想通貨が機能する仕組み』（日経BP社・2016年）〔Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press 2016〕225-233頁。

い[12]」ことが指摘されている[13]。仮想通貨の法的性質決定が実務上の具体的問題を解決する決め手にならないとすれば――既存の法概念との整合性（裁判手続における採用の容易さ）などの点で議論の必要性が否定されないとしても――その意義を問い直す必要があるように思われるのである。

以上のような事情が存在するにもかかわらず、本稿が、ビットコインに代表される仮想通貨の法的性質を取り上げるのは、この問題に関する従前の議論状況が、法とプログラム・コードの関係を考えるうえで、興味深い題材といえるからである。仮想通貨はプログラム・コードによって規定される一種のアーキテクチャである。プログラム・コードやアーキテクチャは――法とは異なる仕方で――人々の行動を規制するものであるが、その内容の正当性や形成過程における正統性について、法の観点から検討する必要性が指摘されている[14]。そこで、仮想通貨の法的性質をめぐる従前の議論を、プログラム・コードに対する法的評価という観点から捉え直すことは――仮想通貨という対象に限定されない――意義を有すると考えられる。また、このような検討は、法の観点から、プログラム・コードの在り方を論じる契機にもなる。この点について、従前の議論には、ビットコインに代表される仮想通貨を所与の前提とする傾向がみられるが、既存の仮想通貨が抱える問題性を、法の観点から明らかにすることも重要であると考えられるのである[15]。

（2） 検討の順序

以下では、まず、法的評価の対象となるプログラム・コードの内容を確認することから始める（**2**）。ビットコインの仕組みについて、法的評価に関連すると考えられる限りで、その内容を紹介する。次に、法的評価の検討に移る（**3**）。プログラム・コードに対する法的評価の在り方という観点から、仮想通貨の法的性質に関する議論状況を整理し、議論の対立点を明らかにしたうえで（**3 (1)**）、ビットコインの取引

(12) 金融法委員会・前掲注 (3) 8 頁。

(13) 末廣③・前掲注 (3) も、仮想通貨の法的性質に関する立場の相違にかかわらず、「多かれ少なかれ、財産権と同じ性質を有すると解されている」(53 頁) と評価し、「個別具体的な場面をどのように解決すべきかがより重要であ〔る〕」(55 頁) とする。

(14) 法とアーキテクチャの関係について、例えば、松尾陽「『法とアーキテクチャ』研究のインターフェース――代替性・正当性・正統性という三つの課題」松尾陽編『アーキテクチャと法――法学のアーキテクチュアルな転回？』(弘文堂・2017 年) 15-30 頁。

(15) このような観点からの検討を行うものとして、小塚荘一郎「仮想通貨に関するいくつかの『大きな』問題」法時 89 巻 11 号 (2018 年) 2 頁。さらに、法、社会規範、市場、アーキテクチャを含む規制の在り方について問題を提起するものとして、片桐直人「貨幣空間の法とアーキテクチャ」松尾陽編『アーキテクチャと法――法学のアーキテクチュアルな転回？』(弘文堂・2017 年) 183-189 頁。

に関するいくつかの法的問題について検討することとする（**3（2）**）。

2　プログラム・コード

ビットコインのプログラム・コードの内容を紹介することから始めよう。プログラム・コードの内容は可変的であることに注意を要するが、以下では、代表的な解説書の説明に従って、法的評価の前提となるプログラム・コードの内容をみていくことにしたい。

（1）ビットコイン・ネットワークとノードの機能

ビットコインはインターネット上の peer-to-peer ネットワーク・アーキテクチャとして構築されている。ビットコイン・ネットワークは、一定のプロトコル（ビットコイン P2P プロトコルや Stratum など）が動作しているノード（node）によって構成される。これらのノードはネットワークにおいて同等の立場を有しており――特別なノードやノードの階層性が存在せず――全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[(16)]。

他方で、それぞれのノードが有する機能は多様である。ビットコイン・ノードの機能には、㋐ルーティング機能、㋑ブロックチェーン・データベース機能、㋒マイニング機能、㋓ウォレット機能が存在する[(17)]。このうち、㋐ルーティング機能は、ビットコイン・ネットワークに参加するための機能である。ネットワークへの参加はノードにとって必須であるため、全てのノードがルーティング機能を有する。これに対して、他の 3 つの機能については、それを有するノードと有しないノードが存在する[(18)]。

まず、㋑ブロックチェーン・データベース機能は、最新かつ完全なブロックチェーンを管理する機能である。そのため、この機能を有するノードは、自律的にビットコイン・トランザクションの検証を行うことができる（**（4）**①参照）。しかし、ブロックチェーン・データベース機能の装備には負担も大きく、2012 年以降、この機能を有しないタイプのノードが導入されている[(19)]。

次に、㋒マイニング機能は、proof-of-work アルゴリズムを解くための機能である

(16)　アントノプロス・前掲注（8）147-148 頁、ナラヤナンほか・前掲注（11）139-140 頁。
(17)　アントノプロス・前掲注（8）148 頁。
(18)　アントノプロス・前掲注（8）148 頁。代表的なノードの種類については、アントノプロス・前掲注（8）150 頁。
(19)　アントノプロス・前掲注（8）155-156 頁。

（（4）③参照）[20]。この機能を備えたノードのことをマイニング・ノード、その保有者をマイナーと呼ぶ。もっとも単にビットコインの取引を行うだけであれば、マイニング機能は必要とされない。実際、現在ではこの機能を備えないノードが多数である。

最後に、㋓ウォレット機能は、ビットコイン・トランザクションを行うための機能である。ビットコイン・トランザクションに際して、記録されているデータ――未使用トランザクション・アウトプット（（3）参照）――の中からインプットに使用するものを選び出すことのほか、秘密鍵、公開鍵、ビットコイン・アドレスの作成が重要な機能といえる。

秘密鍵は、ランダムに選択された数値であり、ビットコイン・トランザクションを行う際の署名の生成に用いられる。ビットコイン・アドレス――秘密鍵を元にして生成される（後述）――と結び付いた未使用トランザクション・アウトプットを利用するために、秘密鍵が必要とされる。それゆえ、秘密鍵を漏洩すると、それを知った他者によってビットコイン・トランザクションがなされてしまうし、秘密鍵を紛失するとトランザクションができなくなる[21]。秘密鍵がビットコイン・トランザクションにおいて決定的な役割を果たすことは、ビットコインの法的性質の検討においても重要な意義を有すると考えられる。

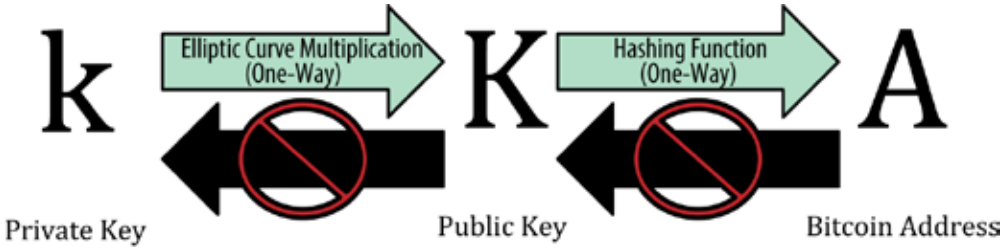
次に、この秘密鍵に基づいて公開鍵が生成される（【図１】参照）。公開鍵は、楕円曲線上のスカラー倍算を用いて、秘密鍵（数値）から計算される楕円曲線上の点として定義される。楕円線上のスカラー倍算は一方向性を有するので、公開鍵から秘密鍵を算出することはできないものとされる[22]。公開鍵はビットコイン・トランザクションを行う際に、相手方に開示される。秘密鍵から一意的に生成される公開鍵と、トランザクションのたびに生成される署名を利用することによって、当該トランザクションの有効性を検証できることになる。

さらに、この公開鍵から、ハッシュ関数を用いてビットコイン・アドレスが生成される（【図１】参照）。ビットコイン・アドレスは、数字の１から始まる文字列である。ハッシュ関数も一方向性を持つため、ビットコイン・アドレスから公開鍵を算出することもできないものとされる[23]。ビットコイン・アドレスは、ビットコイン・トランザクションを行う際の「名義」というべきものであり、取引相手に広く公開され

(20)　アントノプロス・前掲注（8）149 頁。
(21)　アントノプロス・前掲注（8）69 頁、ナラヤナンほか・前掲注（11）155 頁。
(22)　アントノプロス・前掲注（8）71-75 頁。
(23)　アントノプロス・前掲注（8）76-77 頁。もっとも、ナラヤナンほか・前掲注（11）149 頁は、ハッシュ関数の暗号解析技術の進展に対する今後の対処の必要性を指摘する。

る。

【図１】



〔出典〕Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media 2014, at 63.

（２）ノードの種類とビットコインの利用者の類型

以上にみた４つの機能の全てを備えたノードのことをフル・ノード（フル・ビットコイン・ノード）と呼び[24]、そのようなノードの保有者をフル・クライアントと呼ぶ[25]。このうち、ビットコイン P2P プロトコルを動作させているリファレンス・クライアント――時期による変動はあるものの 5,000 ～ 10,000 とされる――が、ビットコイン・ネットワークの中核を構成する。

他方で、多くのノードは４つの機能の１つ又は複数を備えない。例えば、単独でマイニングのみを行うためにネットワークに参加するノード――その保有者はソロ・マイナーと呼ばれる――は、ルーティング機能、ブロックチェーン・データベース機能、マイニング機能を有するものの、ウォレット機能を有しない[26]。また、proof-of-work に多大な計算力が必要とされるようになった今日では、単独でマイニングを行う者は少数になっており、多くのマイナーはグループで協力してマイニングを行っている（マイニング・プール）。そのようなマイナーのノードは、ルーティング機能とマイニング機能のみを有する。ブロックチェーン・データベース機能については、グループ内の他のノードに依存するのである[27]。

ビットコインを取引のために利用するネットワーク参加者の多くは、マイニングを行うわけではない。そのような参加者のノードは、ルーティング機能とウォレット機能のみを有する。このようなノードを、軽量（light weight）ノードや SPV（simpli-

(24)　アントノプロス・前掲注（8）148-149 頁・155 頁。
(25)　アントノプロス・前掲注（8）6 頁。
(26)　アントノプロス・前掲注（8）150 頁。
(27)　アントノプロス・前掲注（8）149 頁・150 頁。

fied payment verification）ノードと呼び[28]、その保有者を軽量クライアントなどと呼ぶ[29]。

フル・クライアントや軽量クライアントは、ノードを保有してビットコイン・ネットワークに参加するが、他人の保有するノードを利用してビットコインの取引を行うことも可能である。例えば、ウェブ・ブラウザを介して他人のサーバにアクセスし、ビットコインの取引を行う利用者は、ウェブ・クライアントなどと呼ばれる[30]。

ビットコインを取引する仕方には様々な態様があるが、現状では、ノードを保有せずにビットコインの取引を行う者が多数に上るといえる。ビットコインの利用者のなかに、ノードを保有してビットコイン・ネットワークに参加する者（以下、「ネットワーク参加者」という）と、ネットワーク参加者を介してビットコインを利用する者（以下、「ネットワーク非参加利用者」という）が存在することは、ビットコインの法的性質を検討するうえでも、重要な意義を有すると考えられる。

（3）ビットコイン・トランザクションの仕組み

続いて、ビットコイン・トランザクションの仕組みについてみていこう。ここで問題となるのは、ネットワーク参加者がウォレット機能を利用してビットコインを取引する場面である。

> 【事例】 事業者Bは取引先であるA1から20.0000BTC、A2から60.0000BTC、A3から30.0000BTCを受領した。Bは取引先であるC1及びC2に対し、それぞれ30.0000BTC、35.0000BTCを支払わなければならないとする。

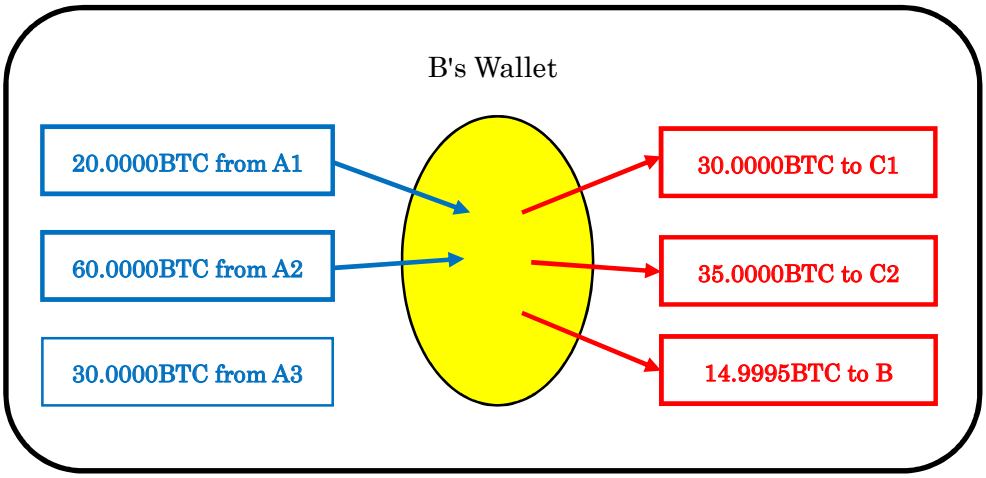
この事例において、Bのノードのウォレット機能は次のように働く（【図２】参照）。まず、Bのウォレットには、未使用トランザクション・アウトプット（UTXO: unspent transaction output）として“20.0000BTC from A1”、“60.0000BTC from A2”、“30.0000BTC from A3”というデータがスクリプトの形で記録されている[31]。Bのウォレットは、これら３つのデータの中から、例えば、“20.0000BTC from A1”、“60.0000BTC from A2”という２つの未使用トランザクション・アウトプットをインプットとして利用することを選択する（この場合、“30.0000BTC from A3”の未使用トランザクション・アウトプットは利用されない）。Bのウォレットは、秘密鍵から

(28) アントノプロス・前掲注（8）150頁・157頁、ナラヤナンほか・前掲注（11）147頁。
(29) アントノプロス・前掲注（8）6頁。
(30) アントノプロス・前掲注（8）6頁。
(31) “20.0000BTC from A1”の“A1”はビットコイン・アドレスのことである。

作られた署名を用いて、未使用トランザクション・アウトプットの拘束条件を解除する。そしてこれら2つのデータから、“30.0000BTC to C1”、“35.0000BTC to C2”、“14.9995BTC to B” という3つのトランザクション・アウトプットを作成する。このトランザクション・アウトプットもスクリプトの形で作成され、受領者（C1、C2、B）のビットコイン・アドレスに対応する秘密鍵から作られた署名を示された場合にのみ、それぞれの受領者が利用できることになる。

なお、インプットとアウトプットを比較すると0.0005BTCの差額が生じていることが分かる。この差額は手数料として当該トランザクションが集積されるブロックのproof-of-workに成功したマイナーに支払われることになる（（4）②参照）。

【図2】



このように、ビットコイン・トランザクションでは、インプットとして利用した未使用トランザクション・アウトプットを――手数料を除いて――全てトランザクション・アウトプットとする必要がある。そのため、B自身に対するトランザクション・アウトプット（“14.9995BTC to B”）の作成が必要になるのである[(32)]。

また、インプットに利用された未使用トランザクション・アウトプットと、それによって作成されるトランザクション・アウトプットとの間には、同一性がない。ビットコイン・トランザクションは、1つ又は複数の未使用トランザクション・アウトプットを利用して、新たに別の1つ又は複数の未使用トランザクション・アウトプットを作り出すものということができる。他方、ウォレット内では、ビットコインの移転元とその額を示すデータが未使用トランザクション・アウトプットの形で存在している。ウォレットに記録されることで、移転元を捨象した残高のみの1つのデータに

(32)　ナラヤナンほか・前掲注（11）118頁。

まとめられるわけではない[33]。これらの点もまた、ビットコインの法的性質の議論において意義を有するものと考えられる。

（4）ビットコイン・トランザクションの承認

次にビットコイン・トランザクションが承認され、ブロックチェーンに記録される仕組み――分散化コンセンサスの仕組み――についてみていこう。

①　個別のトランザクションの検証

あるビットコイン・トランザクションが行われると、そのデータは他のノードに送られる。データを受け取ったノードは、一定のチェック・リスト[34]――トランザクションの構文とデータ構造が正しいか、インプットとアウトプットのいずれも空でないかなど――に従って当該トランザクションのデータとしての有効性を検証する。この検証によって無効と判断されたトランザクションは、検証を行ったノードによって破棄される[35]。

②　トランザクションの候補ブロックへの集積

有効性を確認されたトランザクションはネットワーク上のメモリ・プール（トランザクション・プール）に一時的に保存される。そして、メモリ・プールに保存されたトランザクションは、マイニング・ノードによる承認を未だ受けていない、あるブロック高の候補ブロック（candidate block）に集積されることになる。この集積には一定の優先順位が存在する。すなわち、インプットの額（value of input）とトランザクションの年齢（古さ）（input age）の積をトランザクションのデータ・サイズ（transaction size）で割ったものを基準として、優先順位が決定される。トランザクションの年齢とは、インプットとして利用される未使用トランザクション・アウト

(33)　アントノプロス・前掲注（8）118-120 頁。本多（1）・前掲注（3）936 頁は、このようなビットコイン・システムの特徴を――「残高管理型」（増額記帳と引落記帳の差額としての残高を管理するタイプ）と「独立管理型」（個々のデータを識別・特定できるタイプ）との対比において――「半独立管理型」と呼ぶ。

もっとも、データ管理の方法に関するプログラム・コードの内容は可変的であり、移転元の情報を捨象した残高のみの 1 つのデータにまとめるタイプの仮想通貨も存在する（Ethereum Community, Ethereum Homestead Documentation, Release 0.1, https://media.readthedocs.org/pdf/ethereum-homestead/latest/ethereum-homestead.pdf, at 66-67 参照）。

(34)　アントノプロス・前掲注（8）188-189 頁。チェック・リストの項目は、新種の DOS 攻撃への対処やトランザクションの種類の増加のために逐次変更される。

(35)　アントノプロス・前掲注（8）119 頁。ある未使用トランザクション・アウトプットが二重に使用された場合の処理については、ナラヤナンほか・前掲注（11）141-142 頁。

プットがブロックチェーンに記録されてから、いくつのブロックが積み重ねられたかを意味する。こうしてより古く大きな額のインプットを持つトランザクションが優先的に選択されることになる[(36)]。

候補ブロック内の一定の容量（50KB）は優先度が高いトランザクションのために留保されている。それゆえ、優先度の高いトランザクションは手数料がゼロであっても、候補ブロックに集積されることになる。マイニング・ノードは、ブロック・サイズの最大値（max block size）までトランザクションを集積する。その際の優先順位はトランザクション手数料をデータ・サイズで割った値を基準とする。それゆえ、手数料ゼロのトランザクションがマイナーによって選択される確率は低くなる[(37)]。現在までのところ、マイナーの報酬は、ブロックのマイニングによるビットコインの取得（コイン・ベース報酬）がその大半を占めており、手数料報酬は重要な意味を有していないため、手数料ゼロのトランザクションが候補ブロックに集積される可能性もある。しかし、コイン・ベース報酬は時間の経過とともに漸減する――21 万ブロックごとにコイン・ベース報酬は半減する――ので、やがてトランザクション手数料がマイナーにとって重要な報酬源になると予想される。この段階に至ると、手数料ゼロ（や低額）のトランザクションが候補ブロックに集積される可能性は極めて低くなる。その結果、これらのトランザクションは、トランザクションの年齢が大きくなり、優先的に処理されるようになるまで、候補ブロックに集積されないことになる。

③　ブロックのマイニング

マイニング・ノードは、候補ブロックにトランザクションを集積し、ブロック・ヘッダを構築した後、当該候補ブロックを有効なものとするために、proof-of-work アルゴリズムに対する解を探索する。この作業をマイニングと呼ぶ。マイニングは、1 つのパラメータを変えながらブロック・ヘッダを繰り返しハッシュ化するプロセスで、出力されるハッシュが特別な条件を満たすまで行われる。大容量の計算能力を利用して、入力をランダムに修正しながら偶然に正しいハッシュを得るまで繰り返し計算を行うことになる[(38)]。

④　ブロックの検証

そうしてマイナーは正しいハッシュを得ると、それを他のノードに伝達する。他の

(36)　アントノプロス・前掲注（8）190-191 頁。
(37)　アントノプロス・前掲注（8）191 頁、ナラヤナンほか・前掲注（11）187 頁。
(38)　アントノプロス・前掲注（8）200 頁、ナラヤナンほか・前掲注（11）198-200 頁。

ノード――マイニング・ノードに限られない――はハッシュの正しさを検証する。proof-of-work アルゴリズムの解（ハッシュ）を見つけるためには多大な計算能力を要するのに対して、いったん正しい解が発見されれば、その解が正しいことを検証するのは容易であり、全てのノードがこれを行うことができる（ハッシュ関数は一方向性を有する）。ハッシュの正しさを確認した他のマイニング・ノードは、同じブロック高のブロックのマイニングを終了し、次のブロック高のマイニングに移ることになる[(39)]。

さらに他のノードは、新しいブロックの有効性――ブロックのデータ構造が構文的に有効であること、ブロックのサイズが受け入れ可能な制限内であること、ブロックに含まれるすべてのトランザクションが検証されていることなど――を検証する。このように他のノードが新しいブロックの有効性を確認することによって、あるブロックのマイニングに成功したノードが不正――自らを受け取り手とする多額のトランザクションをブロックの中に潜ませておくことなど――を行うのを防ぐことができる[(40)]。

⑤　ブロックチェーンの再構成とフォーク

ブロックチェーン・データベース機能を有するノードが、あるブロックの有効性を確認すると、当該ノードが有する既存のブロックチェーンに当該ブロックを結び付けて、ブロックチェーンを再構成することになる。あるノードが有するブロックチェーンはメイン・チェーンとセカンダリー・チェーンに区別される。メイン・チェーンは最も多くのブロック――正確には最も多くの累積 difficulty――を有するチェーンであり、そこから分岐したチェーンのことをセカンダリー・チェーンと呼ぶ[(41)]。

ブロックチェーンは分散化しているので、各ノードが有するブロックチェーンのデータが常に一致するわけではない。とりわけ問題となるのが、複数のマイナーが候補ブロックのマイニングを競争するのが通常であるために、ほぼ同時に複数のマイナーが proof-of-work アルゴリズムの解を見つける可能性があることである。この場合、正しい解を見つけたマイナーは、その解をそれぞれ別々に他のノードに伝達する。その結果、一時的にノード間で異なるブロックチェーンを有するという事態が生じる。これをブロックチェーンのフォークと呼ぶ[(42)]。

---

(39)　アントノプロス・前掲注（8）189-190 頁。
(40)　アントノプロス・前掲注（8）210-211 頁。
(41)　アントノプロス・前掲注（8）211-212 頁。
(42)　アントノプロス・前掲注（8）213 頁。

フォークが生じた場合、それぞれのノードは、自らが最初に構築したブロックチェーンをメイン・チェーンとして、そこに新しいブロックを組み込んでいくことになる。他方で、別のバージョンのブロックチェーンも、セカンダリー・チェーンとして保有する。そうして、その後にどちらのチェーンに対して、マイナーがより多くのブロックを追加するかを見守る。もしセカンダリー・チェーンの方が多くのブロックを獲得することになった場合には、そのブロックチェーンをメイン・チェーンに変更することになる。このようにブロックの長さに基づいてメイン・チェーンが変更されることを、ブロックチェーンの再収斂（reconvergence）と呼ぶ。フォークが生じるのは通常1ブロックについてのみであり（2ブロック分のフォークが生じるのはまれである）、多くの場合は10分程度で解消されることになる。採用されなかったブロックチェーンに組み込まれたブロックは解消され、そこに含まれていた個別のトランザクションは次のブロックによる集積の対象となる[(43)]。

以上のように、どのブロックチェーンがメイン・チェーンとして存続するかは、どのブロックチェーンがより多くのマイナーによって選択されるかに依存する。その結果、多くの計算能力を有するマイニング・ノード（マイニング・プール）が協力すれば、故意にフォークを生み出し、自らが作り出したチェーンへの再収斂を生じさせることによって、あるブロックとそこに含まれるトランザクションを無効にすることができる。この問題は51％攻撃などと呼ばれている[(44)]。

ビットコイン・トランザクションは、以上のようなプロセスを経てネットワーク内において承認されることになる。このような承認の仕組みを、法的にどのように評価すべきかが問題となるのである。

３　法的評価

以上に説明したプログラム・コードの内容について、それを法的にどのように評価するかという観点から、従前の議論状況について検討することにしよう。

(43)　アントノプロス・前掲注（8）213-218頁。

(44)　アントノプロス・前掲注（8）224-227頁。もっとも、ビットコイン・ネットワークを構成する計算能力の51%を支配することは、必ずしも必要でない。

（1）従前の議論状況

① 議論の前提

a 資金決済法の定義規定の性格

従前の議論では、いくつかの前提が共有されている。まず、資金決済法における仮想通貨の定義規定の性格についてである。資金決済法2条5項は、「仮想通貨」を「物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。…）であって、電子情報処理組織を用いて移転することができるもの」（1号）、及び「不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの」（2号）と定義する。この「財産的価値」という文言が示す通り、資金決済法の定義規定は、仮想通貨の私法上の法的性質について特定の立場を採用するものではないと理解されている[(45)]。立案担当者によれば、この定義規定は、金融活動作業部会（Financial Action Task Force; FATF）のガイダンスにおける仮想通貨の定義[(46)]を参考にしたものとされており[(47)]、現実社会において仮想通貨が果たしうる機能に着目して、仮想通貨の意義を定めるものといえる。従前の議論においても、資金決済法の定義規定は、仮想通貨の私法上の法的性質を明らかにするものではないという点では、見解の一致をみるのである[(48)]。

---

(45) 末廣①・前掲注（3）73頁、末廣②・前掲注（3）67-68頁、末廣③・前掲注（3）52-53頁、森田・前掲注（3）14-15頁、金融法委員会・前掲注（3）1頁注3。

(46) The Financial Action Task Force, Guidance for a Risk-based approach to virtual currencies, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (2015) at 26は、仮想通貨を「デジタルに取引をすることができ、かつ、⑴交換手段（medium of exchange）、⑵計算単位（unit of account）、及び／又は⑶価値保蔵（store of value）として機能するデジタルな価値の表象（digital representation of value）」とする。

(47) 佐藤監修・前掲注（5）35頁。

(48) この点に関連して、資金決済法2条7項は、「仮想通貨の交換等」を「仮想通貨の売買又は他の仮想通貨との交換」（1号）及び「前号に掲げる行為の媒介、取次ぎ又は代理」（2号）と定義する。しかし、資金決済法は、仮想通貨の私法上の法的性質を明らかにするものではないことから、同項1号にいう「売買」や「交換」は「民法上の売買や交換に該当するものである必要はなく、経済的に、法定通貨を用いて仮想通貨を取得している、逆に、仮想通貨を用いて法定通貨等を取得していると評価できるような取引を指すと考えるべきである」ことが指摘されている（森下・前掲注（3）794頁）。

b　所有権・債権概念等への該当性の否定

また、近時の実務・学説の議論では、ビットコインに代表される仮想通貨が一定の法概念に該当しないことについて――異論は存在しうるものの――共通理解が形成されつつあることを指摘できる。

まず、ビットコインはデータとして存在するにすぎず、有体性を欠くために、民法上の物（民法85条）には該当しない(49)。それゆえ、所有権の客体が物（有体物）に限られるという一般的な理解（民法206条参照）を前提とすれば(50)、ビットコインを客体とする所有権（民法206条）を観念できないことになる(51)。他方、ビットコインに知的財産権（無体財産権）を認めることについても――その根拠となる法律が存在しないことに加え(52)――そもそもビットコインが情報財としての性格を有しないことを理由として、消極的に解されている(53)。さらに、ビットコインは発行者の存在を前提としないため(54)、前払式決済手段（資金決済法3条1項1号）と異なり、発行者を債務者とする債権と構成することもできないとされる(55)。

以上の理解を前提として、既存の法概念との関係で、ビットコインの私法上の位置

(49)　もっとも、田中＝遠藤（上）・前掲注（3）59頁注17は、無記名債権に関する民法86条3項を類推適用することによって、仮想通貨を「モノ」として扱う可能性を示唆する。

(50)　ただし、学説上は「法律における『有体物』を『法律上の排他的支配の可能性』という意義に解し、物の観念を拡張すべき」とする有力な見解が存在する（我妻栄『新訂民法総則（民法講義Ⅰ）』〔岩波書店・1965年〕202頁）。

(51)　芝①・前掲注（3）86頁、末廣①・前掲注（3）73頁、末廣②・前掲注（3）68頁、末廣③・前掲注（3）53頁、後藤＝渡邉（総論）・前掲注（3）114-115頁、森田・前掲注（3）15頁、金融法委員会・前掲注（3）4頁。また東京地判平成27年8月15日（前掲注（4））は、ビットコインの有体性及び排他的支配可能性の欠如を理由として、ビットコインに対する所有権の成立を否定し、Mt. Gox社の破産手続における顧客の取戻権を否定した。

　なお、ドイツ法においても、ビットコインが民法上の物（ドイツ民法90条）の性質を有しないことから、ビットコインに対する所有権（ドイツ民法903条以下）を観念できないことが指摘されている（Gerald Spindler und Martin Bille, Rechtsprobleme von Bitcoin als virtuelle Währung, WM 2014 Heft 29, S. 1359）。

(52)　後藤＝渡邉（総論）・前掲注（3）115頁、武内・前掲注（3）16頁。

(53)　森田・前掲注（3）15頁、本多（2・完）・前掲注（3）1196-1198頁。また、西村あさひ法律事務所編・前掲注（3）843頁〔芝章浩〕も、ビットコイン取引の検証作業（マイニング）により「思想が創作的に表現されていると評価することは困難であろう」とする。

(54)　第186回国会答弁（内閣参質186第28号）も「ビットコインについては、特定の発行体が存在せず、各国政府や中央銀行による信用の裏付けもない等の特徴を有するとされている」とする。

(55)　田中＝遠藤（上）・前掲注（3）59頁、片岡①・前掲注（3）33頁、武内・前掲注（3）15頁、末廣①・前掲注（3）73-74頁、末廣②・前掲注（3）68頁、日本銀行決済機構局・金融研究所・前掲注（3）8頁、末廣③・前掲注（3）53頁、後藤＝渡邉（総論）・前掲注（3）115頁、森田・前掲注（3）15頁、金融法委員会・前掲注（3）4頁。同様の議論は、ドイツ法にも存在する（Spindler und Bille, a.a.O. Fn. 51, SS. 1359-1360）。

づけをいかに解するかが問題とされるのである。

② 議論の対立点

a ビットコインに対する権利性を否定する立場

まず、ビットコインに対する権利性を否定する見解が存在する(56)。代表的な論者は「ビットコインの保有は、秘密鍵の排他的な管理を通じて当該秘密鍵に係るアドレスに紐づいたビットコインを他のアドレスに送付することができる状態を独占しているという事実状態にほかならず、何らかの権利または法律関係をも伴うものではないと考えられる(57)」と説明する(58)。そして、そのように解したとしても、ビットコインの取引には当事者間の契約を観念できるし(59)、ビットコインの独占的保有という事実状態は不法行為法・刑法などの保護の対象となることを指摘する。さらに、ビットコインに対する権利性を認めないことにより――とりわけ原因関係の不存在・瑕疵に基づく物権的返還請求権が否定されることを理由として――決済手段としての安定性・有用性が確保されるとするのである(60)。

(56) 早くからこのような立場を主張していたものとして、片岡①・前掲注（3）29頁は、ビットコインに代表される仮想通貨を「あらかじめ定められた規範に基づき、この規範を承認する不特定の参加者によって管理し、使用される電磁的記録であって、それらの者の間で数量的単位を有する財産的価値を表象するもの」と説明する（もっとも、論者はその後、ビットコインについて「物権又はいわゆる準物権と同様の構造」を肯定する形で議論を展開するに至る（片岡③・前掲注（3）14頁））。また、後藤＝渡邉（総論）・前掲注（3）115頁も「利用者による利用者アドレス宛出力データの排他的『利用』は、利用者に帰属する何らかの財産権により確保されうるものではなく、利用者が、利用者アドレスの秘密鍵を事実上利用者のみが独占的に利用できる状態で管理すること（…）により、事実上達成されるものである」とする。

(57) 西村あさひ法律事務所編・前掲注（3）845頁〔芝章浩〕。芝①・前掲注（3）86頁も同旨。

(58) このような考え方は、比較法的に孤立したものではなく、ドイツでは有力な見解といえる。例えば、Benjamin Beck und Domik König, Bitcoins als Gegenstand von sekundären Leistungspflichten: Erfassung dem Grunde und der Höhe nach, AcP 215 (2016) SS. 659-660は、ビットコインについて法的意味における処分が可能な地位を観念することはできず、他人に対してビットコインの移転を請求する権利を有する者は、一定額のビットコインのデータにアクセスする事実上の排他的地位（eine faktisch exklusive Position）を有するにすぎないとする。

(59) もっとも、ビットコインに対する財産権を認めないことから、ビットコインの取引に関する契約は、「財産」を対象とする贈与契約（民法549条）には該当しうるものの、「財産権」を対象とする売買契約（民法555条）には該当しないとの解釈論が展開される。そのうえで、有償でのビットコインの取引は、一種の役務提供契約として、売買契約の規定が準用される（民法559条）ものと説明される（西村あさひ法律事務所編・前掲注（3）853-854頁〔芝章浩〕）。

(60) 芝①・前掲注（3）88頁、西村あさひ法律事務所編・前掲注（3）844頁・852頁〔芝章浩〕。得津①・前掲注（3）163頁も、無権限取引を念頭に置いて、仮想通貨を金銭や物に準じたも

以上の見解の前提には、「秘密鍵を利用した送付などのビットコインの仕組みはビットコインのプロトコルを事実的な根拠として成立しているのであって重ねて規範的な根拠を観念する必要はない[61]」という理解が存在している[62]。プログラム・コードに対する法的評価という観点からすると、この見解は、プログラム・コードによって規律される領域について法的評価を行うことに消極的な態度をとるものということができる。

この点を推し進めれば、プログラム・コードに対する法的評価を敢えて避けるという立場もありうる[63]。もっともこの立場は、ビットコインの利用者に対する法的保護の否定を意味するのであり、ビットコインの利用を抑制する効果を持つことになる[64]。

しかし、そのような帰結は前述した論者の意図とは異なる。ビットコインに対する権利性を否定することで、決済手段としての利用を促進することが目指されていたからである。その意味で、ビットコインの権利性を否定する見解は、ビットコインのプログラム・コードを法的に評価することの困難さを指摘するにとどまり、法的評価それ自体に対して否定的な態度をとるわけではないと考えられる[65]。

さらに、この見解も、個別の法律問題との関係で、ビットコインの帰属について規範的評価が必要となる場合があることを認めている[66]。そうだとすれば、ビットコインの前提とするプログラム・コード自体について、それを法的評価の対象から除外する理由は乏しいものと考えられる[67]。

のとして扱うよりも、当事者間の役務提供契約として理解する（仮想通貨に対する権利性を否定する）方が、決済手段としての利用が促進されることを指摘する。

(61) 西村あさひ法律事務所編・前掲注（3）845 頁〔芝章浩〕。

(62) なお、片岡①・前掲注（3）は、ビットコインに代表される仮想通貨について「規範」の「承認」を語るが（29 頁）、そこでいう「規範」とはプログラム・コードとしての「ルール」を意味し、ビットコインに関する当事者の関係を「事実状態」と表現する（33 頁）。

(63) 得津①・前掲注（3）155 頁が「リヴァイアサン的な自然状態」と称する状態を承認する立場である。

(64) 得津①・前掲注（3）163 頁。

(65) 芝②・前掲注（3）51-52 頁も、決済手段としての利用促進の観点から、物権的返還請求権を否定する見解として、ビットコインに対する権利性を否定する見解のほか、権利性を肯定する見解のうち一定の立場（後述する第 2・第 3 の見解）を並列して紹介する。

(66) 西村あさひ法律事務所編・前掲注（3）845-847 頁〔芝章浩〕、芝②・前掲注（3）51 頁。なお、片岡①・前掲注（3）36 頁は、仮想通貨が決済手段として用いられる場合について、商品との交換契約（民法 586 条 1 項）や、仮想通貨による金銭債務の弁済の合意を代物弁済（民法 482 条）と性質決定すべきものとする。

(67) 森田・前掲注（3）23 頁は、仮想通貨が決済手段として用いられる場合を念頭に、「単なる事実状態のみによって決済手段を説明することは、論理的に困難である」とする。仮想通貨に決済手段としての性質が認められる根拠を明らかにするために、法的評価が必要であること

b　ビットコインに対する権利性を肯定する立場

次に、ビットコインに対する権利性を肯定する立場についてみていこう。近時の整理によれば、3つの見解が対立するものとされる。すなわち、「物権又はこれに準ずるもの」を認める見解（(a)）、「財産権を認める」見解（(b)）、及び「プログラム・コードに対する合意（同意）を根拠」とする見解（(c)）である[68]。もっとも、これらの見解の対立点がどこにあるのかについては、慎重な検討を要する。

(a)　物権又はこれに準ずるものを認める見解

第1の見解からみていこう。この立場に分類される代表的な論者は「仮想通貨は、日本の私法上、法的保護に値する財産的価値であり、そうした財産的価値として法的にも権利の対象や取引の対象として扱われるべきものであってその帰属や移転については、原則として物権法のルールに従うと考えるべきである[69]」とする。もっともここで言及される「物権法のルール」とは、ペーパーレス化された有価証券の取引のほか、預金（預金債権）の帰属をも射程に含むものと説明されるので[70]、その限りでは、第2の見解（財産権を認める見解）と大きな違いはないと評価することもできる。

他方――第2の見解と比較した場合の――第1の見解の特徴は、「仮想通貨の帰属や移転については、一次的には帳簿や台帳の記録を手掛かりとしつつ、そこで権利者として記録されている者が本来の権利者でない場合には、本来の権利者に帰属させることが望ましい[71]」という価値判断に求められる。それゆえ、「本来の権利者」は「権利者として記録されている者」に対して、仮想通貨の返還を内容とする物権的請求権を有することになるものと解される[72]。

このような見解の前提には――本稿の冒頭でも指摘した――ビットコインに代表される仮想通貨が「決済手段として用いられることは少なく、投資の対象として保有されている割合の方がはるかに多いようである[73]」という現状を重視する姿勢があるものと考えられる。このことは、仮想通貨の「利用実態が通貨に近い状態である場合に

を指摘するものといえる。

(68)　金融法委員会・前掲注（3）6頁（同8-11頁において、それぞれの見解の当否が検討される）。同様の分類は末廣③・前掲注（3）53-55頁に採用されるほか、芝②・前掲注（3）50-52頁も、物権的返還請求権を肯定するか否かという観点から類似の整理を行う。

(69)　森下・前掲注（3）807頁。

(70)　森下・前掲注（3）807-808頁。

(71)　森下・前掲注（3）808頁。

(72)　金融法委員会・前掲注（3）13頁、芝②・前掲注（3）50頁参照。

(73)　森下・前掲注（3）786頁。

は、通貨や外国通貨に関する私法ルールの準用も考えられよう[74]」という指摘にも現れている[75]。第1の見解は、仮想通貨の利用の実態を念頭において適切なルールを選択すべきという実質的論拠に基づくものということができる[76]。

この点で、第1の見解は、他の見解の多くが、決済手段としての利用を念頭に置いて、ビットコインに代表される仮想通貨の法的性質を論じるのと異なる。そして、仮想通貨の決済手段としての性質が、その前提とするプログラム・コードに由来することに鑑みれば、第1の見解は、プログラム・コードの内容から離れ、現実社会における利用実態に着目して、仮想通貨に対する法的評価を行うものということができる。法的評価に際して、プログラム・コードの内容から距離をとるところに、第1の見解の特徴があると考えられるのである。

(b) 財産権を認める見解

次に、第2の見解は、ビットコインに代表される仮想通貨に対する財産権を肯定する。しかし、この見解の主眼は――財産権の肯定それ自体というより――仮想通貨に決済手段としての性質を認める点にあると考えられる。

第2の見解の代表的論者は、民法上の「財産権」概念が「処分することを得べき利益を目的とする権利」を意味することを前提として、「一定の利益が『財産権』として法主体に排他的に帰属することにより、この者に認められる法的権能が『処分権』であると捉えることができる[77]」と説明する。この説明は、事実上、ある主体がある対象に関する排他的支配可能性を有する場合に、その状態を、法的に、財産権の帰属と評価するものと理解される。そして、当該主体は自らに帰属する財産権を法的に処分する権限（処分権）を有するものとされる。以上の理解によれば、ブロックチェーン技術の登場により――従前は困難とされていた――特定の主体が仮想通貨に関するデータを排他的に支配できるという事実状態が生じたことが、仮想通貨に対する財産権を肯定する決定的要因であるということになる[78]。仮想通貨のデータを排他的に支

(74) 森下・前掲注（3）808頁注118。

(75) もっとも、預金の帰属に関する論者の従前の見解（岩原紳作＝森下哲朗「預金の帰属をめぐる諸問題」金法1746号（2005年）36-39頁）によれば、ビットコインが決済手段として利用される実態がある場合にも、直ちに「物権法のルール」の適用が排除されるという帰結は導かれないように思われる。

(76) 以上と比較すると――同じく第1の見解に分類されることの多い（金融法委員会・前掲注（3）6頁注20）――片岡③・前掲注（3）15頁は、仮想通貨の「準物権的構造」に基づいて、仮想通貨の取引がなされた場合に「物権的及び物権変動的な支配移転請求権」を肯定するものの、そこでの問題関心は論者の前提とする法概念上の整合性に向けられているようにみえる。

(77) 森田・前掲注（3）16頁

(78) 本多（2・完）・前掲注（3）1202頁は――第2の見解が前提とする財産権概念を共有するか

配できる事実状態に着目する点では、仮想通貨に対する権利性を否定する見解と共通するが、そのような事実状態について財産権の帰属という法的評価を付与する点に[79]、第2の見解の特徴があるといえる。

もっとも、仮想通貨に対する財産権を肯定することから導かれる法的帰結は――当該財産権が帰属主体の責任財産に属することや相続の対象となることのほか――財産権の帰属変更について所有権移転と同様の規律が妥当することや、財産権の帰属に対する侵害があった場合に所有権に基づく返還請求権と同様の規律が妥当することである[80]。このような帰結は、第1の見解の主張する内容と重なることになる[81]。しかしながら、第2の見解の主眼は、以上の帰結を否定する――仮想通貨の帰属・移転について財産権に関する規律が妥当しないことを主張する――点にあるといえる。そのために、第2の見解は、仮想通貨の決済手段としての性質に着目するのである。

まず、決済手段の代表である金銭は「特定の通貨単位の数額として表示されたところの『価値的権能』」と定義される。金銭債務の目的は――金銭を表象する有体物（紙や金属）の移転ではなく――この価値的権能の移転であり、金銭債務を消滅させる価値的権能は「支払単位」と呼ばれる。もっとも、支払単位は抽象的な価値であるため、それを特定の主体に排他的に帰属する状態を創り出す必要がある。そこで「社会において一定の支払単位が組み込まれたものとして合意され、かつ、それを通じて価値の帰属を実体的にトレースすることを可能とするような一定の媒体」（「通貨媒体」）が必要とされる。また、通貨媒体に表象された支払価値を移転するための手段（「通貨手段」）も要請される。第2の見解は、金銭に代表される決済手段は「それを構成する『通貨媒体』と『通貨手段』との組合せによって法的に把握することが可能となる」と説明するのである[82]。

以上の理解を前提として、決済手段としての仮想通貨については、通貨媒体と通貨

否かは明らかでないものの――「ブロックチェーンという新たな技術の登場によって、他の方法では不可能であった排他的帰属を決定し、また、それを移転させることが可能となり、それゆえに『価値』を財産・財産権と捉えることが可能になったといえるのではないか」と指摘する。仮想通貨というデータの事実上の排他的支配を可能とする点に、ブロックチェーン技術の法的意義を見出す立場と評価することができる。

(79) 第2の見解の前提とする「財産権」概念については、法律に規定が存在せず（金融法委員会・前掲注（3）9頁）、実定法の議論の前提とすることができないとの批判がある（片岡⑤・前掲注（3）9-10頁）。この点については――民法の規定に「財産権」という文言が存在することをいかに評価するかという点に加えて――議論の前提とされる「財産権」概念に関し、論者の間に理解の相違があることを指摘すべきように思われる。

(80) 森田・前掲注（3）16-17頁。

(81) 森田・前掲注（3）17頁。

(82) 森田・前掲注（3）18頁。

手段の双方が「ブロックチェーンにおける取引記録によって実現されている[83]」と評価される。まず、通貨媒体については、利用者の特定のアドレスに取引記録が集積されることを前提として、当該アドレスに対応した秘密鍵の存在により、仮想通貨の排他的帰属が可能になるものと説明される。また通貨手段については、利用者が行った取引がブロックチェーン上に記録されることによって、仮想通貨の移転が実現されるものとされるのである[84]。

このように、第2の見解は、ビットコインのプログラム・コードの内容を、法的に通貨媒体及び通貨手段と評価することで、仮想通貨の決済手段としての性格を基礎づけるものといえる[85]。プログラム・コードに対する法的評価を通じて、仮想通貨の法的性質を明らかにしようとする点に――仮想通貨に対する権利性を否定する見解と比較した場合の――第2の見解の特徴があると考えられる。

他方、第1の見解と比較した場合には、法的性質決定に際して、ビットコイン取引の実態よりも、ビットコインのプログラム・コードの内容を重視する点に、第2の見解の特色がみられる。また、第2の見解が前提とする通貨媒体の概念が「社会において一定の支払単位が組み込まれたものとして合意され〔た〕」ものであることからすれば、決済手段という性質決定の前提として、仮想通貨の利用者（「社会」）がプログラム・コードの内容について有する認識（「合意」）も、重要な問題ということができる。そしてこれらの点は、次にみる第3の見解の問題意識と共通するものと考えられるのである。

(c) プログラム・コードに対する合意（同意）を根拠とする見解

第3の見解は、プログラム・コードに対する合意（同意）を根拠として、仮想通貨に対する権利性を肯定する。代表的論者は、「ビットコインの保有を可能にしているのは、取引参加者全員が『合意』し、前提としている仕組み（またはプロトコル）であり、そのような合意が一種のソフトローとなってシステム全体を支えていると言えよう[86]」とする。ビットコインの取引に参加する者の間に合意の存在を認めることで、参加者が有する法的地位を参加者相互間の権利義務関係として把握する立場であるということができる。もっとも、そこでの参加者の「合意」については、「個々の当事者間で結ばれる相対の契約のようなイメージのものではなく、参加者全員が従う

(83) 森田・前掲注（3）20頁。
(84) 森田・前掲注（3）20-21頁。
(85) 本多（2・完）・前掲注（3）1198-1202頁も、本文で紹介した論者の見解を「無体物の占有理論」と称したうえで、それに基づいてビットコインの法的性質を説明すべきことを主張する。
(86) 末廣②・前掲注（3）68頁。末廣①・前掲注（3）74頁も同旨。

ことに合意している規範のようなものである[87]」という留保が付される。そしてそれゆえ、当該合意は「伝統的な民法（契約法）の世界で考えられている合意や契約と異なるものと考えざるを得ない」とされ、「そのような希薄な『合意』により、本来の意味での合意や契約と同じような拘束力を認めることができるかが理論的な検討課題である」ことが指摘されるのである[88]。

このため、第3の見解に対しては、ネットワーク参加者の合意を契約と性質決定することができず、契約（合意）に基づく地位として、仮想通貨に対する権利性を説明することができないという――論者によって予想されていた――批判が向けられることになる[89]。もっとも、そこでの批判の根拠が合意の「希薄さ」にあるのだとすれば、それだけでは批判として十分とはいい難い。現実の社会には、約款取引をはじめとして、希薄な合意に基づく契約（当事者が権利義務関係を十分に認識することなく締結される契約）が多数存在している。他方、第3の見解が合意の主体としてネットワーク参加者を想定する――ネットワーク非参加利用者を除外する――のであれば、それらの者は、ノードを新たに保有することでビットコイン・ネットワークに参加しており、ビットコインのプログラム・コードの内容にも一定の理解を有しているものと想定することができる。それゆえ、ネットワーク参加者の合意が、約款取引などと比較して特に希薄であるとは言えないように思われる。また、仮に、ネットワーク参加者の合意が希薄であると評価するとしても、むしろ問題は、そのような希薄な合意に基づく契約について、法がいかに対処すべきか、である。その意味で――論者も指摘するように――ネットワーク参加者の合意という考え方は、契約という法概念に課題を提起することになる。もっとも、この点については、既に一定の議論の蓄積が存在するところであり、それ自体が新しい課題というわけではない。

このように考えると、第3の見解に対する批判として重要なのは、代表的論者が、合意の内容を「コードに対する合意」と表現する点であるように思われる。参加者がビットコインのプログラム・コードの内容に同意してビットコインを利用しているという事態が存在するとしても、その事態を、法的にいかなる合意と評価すべきかは、別次元の問題である[90]。それゆえ、プログラム・コードの内容を、当事者の法的な権

(87) 末廣②・前掲注（3）69頁注9。

(88) 末廣③・前掲注（3）55頁。

(89) 西村あさひ法律事務所編・前掲注（3）845頁〔芝章浩〕、日本銀行決済機構局・金融研究所・前掲注（3）8頁、片岡④・前掲注（3）163頁、森田・前掲注（3）22頁、金融法委員会・前掲注（3）10-11頁、片岡⑤・前掲注（3）12頁。ドイツ法にも類似の議論が存在する（Spindler und Bille, a.a.O. Fn. 51, S. 1360）。

(90) 森田・前掲注（3）23頁は、法とプログラム・コードが「階層を異にする規範である」ことを指摘する。

利義務関係として評価し直すことが必要になるのである。

この点について、第3の見解は、プログラム・コードの内容を、可能な限り法的評価に反映させることを目指す立場であると考えられる。実際、第3の見解の前提には、「仮想通貨の取引ルールは、ネットワーク参加者が前提としている仕組みを最大限尊重すべきである[(91)]」という判断が存在する。そして、法的評価において、プログラム・コードの内容に適合的な法律構成を採用すべきという立場を前提とすれば、当事者の合意という法律構成が有する柔軟性に積極的な意義が見いだされるのである[(92)]。

ただし、当事者の合意という構成を採用することで、プログラム・コードの内容と法的評価が一致するわけではないことには注意を要する。法的評価においては、当事者の合意に対する制約が問題となりうるからである。第3の見解も「契約法に関して内容・手続を制約するルール（民法90条の公序良俗違反による無効、消費者契約法や約款論等）との関係が問題となる可能性[(93)]」を指摘する。その意味で、法的評価における修正の余地を認めつつ、可能な範囲で、プログラム・コードの内容を尊重すべきというのが、第3の見解の基本的な立場であると理解することができる。

③　議論状況の評価

以上の検討によれば、従前の議論の対立は、見かけほど大きなものではないことが分かる。

まず、仮想通貨に対する権利性を否定する見解は、仮想通貨の決済手段としての利用の促進を目指すのであり、その点では、仮想通貨に対する権利性を肯定する立場のうちの第2・第3の見解と軌を一にする。権利性を否定する根拠は、ビットコインのプログラム・コードを法的に評価することの困難さに求められるのであり、法的評価それ自体に対して否定的な態度がとられているわけではない。そして、プログラム・コードの内容の正当性や形成過程における正統性について、法の観点からの検討が要請されることを前提とすれば、ビットコインのプログラム・コードに対する法的評価の必要性を肯定できるものと考えられる。

次に、法的評価に際して、プログラム・コードの内容を、どの程度尊重すべきかが問題となる。仮想通貨に対する権利性を肯定する立場のうち、第2・第3の見解が決

(91)　末廣①・前掲注（3）74頁。末廣②・前掲注（3）68頁も同旨。

(92)　末廣③・前掲注（3）55頁は、「世の中では様々な仮想通貨が生み出され、…それぞれが異なる特徴を有している」という現状を踏まえて、当事者の合意という法律構成の「応用可能性」に利点を見出す。

(93)　末廣②・前掲注（3）73頁。

済手段として用いられることを前提としたプログラム・コードの内容を重視するのに対して、第１の見解はビットコインの取引の実態に即した法律構成を採用すべきことを主張する。この点で、第１の見解には、プログラム・コードの内容に対する批判的な法的評価としての性格が色濃く現れることになる。もっとも、プログラム・コードの内容に即した法律構成を採用したうえで、その内容を批判的に検討することも可能である。むしろ、批判を有効なものとするためには、プログラム・コードの内容を尊重する形で法的評価を試みることが望ましいとも考えられる。

このように考えた場合、ビットコインのプログラム・コードの内容を法的評価に反映させるために、ネットワーク参加者の合意という法律構成を採用すべきである、という第３の見解の主張が注目に値する。この主張は、第２の見解にも通底するものといえる。前述の通り、第２の見解は、プログラム・コードの内容に着目して、ビットコインに決済手段としての性質を肯定するが、そこでは、ビットコインの利用者が、ビットコインの仕組みにいかなる認識を有しているかが重要な意義を有するものと解されるからである。また、第３の見解については、仮想通貨の法的性質をネットワーク参加者の合意で説明するとしても、合意の内容をいかに理解するかによって法的帰結が異なることになるので、他の見解とは「異なる次元の議論である(94)」との指摘がある。つまり、ネットワーク参加者の合意に対する法的評価の内容次第で――第２の見解の主張する――決済手段としての性質を、ビットコインに肯定することもできるのである。

さらに、ネットワーク参加者の合意という観点からプログラム・コードの内容を評価することは――後述のように――プログラム・コードが抱える法的な問題点を指摘することにもつながる。このような考慮に基づいて、以下では、ビットコインに代表される仮想通貨の法的性質を、ネットワーク参加者の合意に基づいて理解する立場から、ビットコインの取引に関連する法的問題について検討することにしたい。

（２）法的問題の検討

前述（２（２））のように、ビットコインの取引を行う者の中には、ネットワーク参加者とネットワーク非参加利用者が存在する。両者の区別は、法的評価においても重要な意義を有する。直前に述べたネットワーク参加者の合意が問題となるのは、主としてネットワーク参加者の法的地位についてである。これに対して、ネットワーク非参加利用者の法的地位については、その者とネットワーク参加者――多くの場合、仮想通貨交換業者――の間の合意が問題となる。後者の合意については――第３の見解

(94)　金融法委員会・前掲注（3）11 頁。

を批判する立場からも――契約と性質決定することに、異論はないものと考えられる。

そこで、以下ではまず、ネットワーク参加者の法的地位について検討したうえで(①)、現実のビットコイン利用者の多数を占めるネットワーク非参加利用者の法的地位についてみていくことにする（②)。

① ネットワーク参加者の法的地位

a 法的地位の内容

ネットワーク参加者は、ビットコインのプログラム・コードに従って、ビットコイン・トランザクションやマイニングなどを行い、その結果を互いに承認しあう関係にある。このような関係を法的に評価すれば、一定のルールに従ってビットコインのデータ（未使用トランザクション・アウトプットなどのデータ）を利用する法的地位を、ネットワーク参加者は相互に有しているものと考えることができる。そして、新たにノードを保有することによって、ビットコイン・ネットワークに参加することは、そのような法的地位に合意したものと評価されることになる。

ビットコインに関する法的地位を以上のように理解する場合、法的地位の内容は、プログラム・コードによって規定されるところが大きくなる。この点で問題となるのが、プログラム・コードの内容が可変的であることである。とりわけ、法的地位の内容に大きな影響を与えるようなプログラム・コードの変更があった場合に――例えば、平成29年夏にビットコインからビットコイン・キャッシュが分裂するというハード・フォークが生じている――そのことをどのように評価するかが問題となる。

1つの考え方としては、ネットワーク参加者の合意が、そもそもプログラム・コードの可変性を前提としており、プログラム・コードの変更によって法的地位の内容が変更されることが、予め合意されているとする立場がありうる。しかし、プログラム・コードの内容の正当性や手続の正統性を法的に評価する必要があることを前提とすれば、このような理解には問題がある。

むしろこの点について参考になるのは、近時の契約法分野における議論の進展である。そこでは、例えば、「特定の当事者同士の契約関係でありながら、一方当事者が、同様な契約を結んでいる他の当事者や、まだ契約関係にない潜在的な当事者への配慮を要求されるような性質の契約」のことを「制度的契約」と呼び、古典的な契約概念（「取引的契約」）と対比する見解が主張されている[(95)]。そして制度的契約の特色として、予め定められた契約内容について当事者が個別に交渉することが認められない一方で（個別交渉排除原則)、潜在的な受給者に財やサービスが平等に提供される

(95) 内田貴『制度的契約論――民営化と契約』（羽鳥書店・2010年）57頁。

こと（平等原則・差別禁止原則）、契約の内容や運用の決定に潜在的な受給者が参加できること（参加原則）、財やサービスの給付の内容や手続について透明性が確保されていること（透明性原則）が要請されることが指摘される[96]。現実の社会における契約の多様性を前提として、一定の性質を有する契約については、古典的な契約とは異なる規範が妥当することが主張されるのである。

このような理解を前提とすれば、ビットコインに関する法的地位の内容を規定するプログラム・コードが変更される場合に、その手続に誰が参加できるか、また、変更の内容や手続に透明性が確保されているか、という視点が導出されることになる[97]。このことは、ビットコインをめぐるガバナンスの問題につながる[98]。既に、「仮想通貨も、将来、社会的に大きな役割を担うようになれば、ルール形成のプロセスに対して緩やかな規制が導入されることは、不可避ではないかと考えられる[99]」との指摘があるが、このことは、契約法学の観点からも正当化されうるのである。そして、仮に、ビットコインのガバナンスに重大な問題があるとすれば、ビットコインに対する法的保護の否定――それは、ビットコインの利用を抑制する効果を持つことになる――が検討されてしかるべきといえる。

以上の可能性を留保しつつ、以下では、現在のビットコインについては法的保護の必要性が認められることを差し当たりの前提として、ビットコインのデータを利用する法的地位[100]について検討することにしたい。

b　法的地位の帰属

まず、法的地位の帰属については、特定のデータを利用する権限を有するのが誰であるかが問題となる。未使用トランザクション・アウトプットについては、前述（**2(3)**）のように、それをビットコイン・トランザクションに利用するために、秘密鍵を用いて拘束条件を解除する必要がある。それゆえ、特定のデータを、秘密鍵を用いて利用できることが、法的地位の帰属の条件となる。

また、未使用トランザクション・アウトプットを利用する前提として、それが含ま

(96)　内田・前掲注（95）86-87 頁。

(97)　この点について、ビットコインのプロトコルの変更には、ビットコイン改善提案（Bitcoin Improvement Proposal）という、誰もが参加可能な手続が存在している（ナラヤナンほか・前掲注（11）292-293 頁）。この手続が十分に機能しているか否かが問題といえる。

(98)　ビットコインのガバナンス及びステーク・ホルダーについては、ナラヤナンほか・前掲注（11）297-300 頁。

(99)　小塚・前掲注（15）3 頁。

(100)　以下の叙述では、ビットコインのデータを利用する法的地位のことを指して、「法的地位」や「ビットコイン」という言葉を用いることがある。

れるビットコイン・トランザクションが承認される必要がある（２（４）参照）。すなわち、当該ビットコイン・トランザクションが検証され、候補ブロックに集積され、当該ブロックが承認を受けることが必要となる。またブロックの承認があっても、ブロックチェーンのフォークが生じ、当該ブロックを含むチェーンがメイン・チェーンとして選択されなかった場合には、そこに集積されたトランザクションは承認されなかったことになり、別途の承認が必要になる。以上を前提とすれば、ビットコイン・ネットワークにおけるトランザクションの承認が、ビットコインのデータ（未使用トランザクション・アウトプット）を利用する法的地位の帰属の前提条件になると解される。その結果、ブロックチェーンのフォークの場面を考えると、一時的にトランザクションが承認を受けたとしても、事後的にその承認が覆され、当該トランザクションに含まれるデータを利用する法的地位の帰属が否定される可能性が存在する。ネットワーク参加者は、その可能性を含めて、法的地位の帰属に関するルールを互いに合意しているものと評価すべきことになる。

このほか、コイン・ベース報酬としてマイナーが取得したデータについても、同様に、その利用に関するプログラム・コードの内容を前提として、法的地位の帰属が判断されるものと考えられる[(101)]。

c　法的地位の移転

(a) 移転の仕組み

次に、ビットコインの移転についてみていこう。ネットワーク参加者は、ビットコイン・トランザクションにより、ビットコインのデータを利用する法的地位を移転することができる。移転の相手方は、ビットコイン・ネットワークにウォレット機能を備えたノードを保有する者に限られる。ネットワーク参加者の間には、法的地位の移転が許容される相手方の範囲に関する合意があるものと考えられる。

以上を前提として問題となるのが、法的地位の移転の手段であるビットコイン・トランザクションが、法的にいかに評価されるかである。前述（２（３））のように、ビットコイン・トランザクションは、１つ又は複数の未使用トランザクション・アウトプットを利用して、新たに別の１つ又は複数の未使用トランザクション・アウトプットを作り出すことを意味する。トランザクションの前後で、未使用トランザクション・アウトプットの同一性は失われることになる。このことを前提とすれば、法

(101) 末廣②・前掲注（3）70 頁は、「マイニングが成功した後に 100 ブロックが生成されない限り、そのビットコインを他者に移転できない」ことを指摘する。末廣①・前掲注（3）76 頁も同旨。

的地位の移転は、移転元のネットワーク参加者の法的地位が消滅し、移転先のネットワーク参加者が新たに法的地位を取得するものと考えることができる。前述した法的地位の帰属に関する説明と併せて考えると、ブロックの検証がなされるごとに、当該ブロックに含まれる多数のトランザクションに基づいた、新しい法的地位の帰属の状態が合意される――更改的効果を有する合意がなされる――ものと評価することができる。このような移転の仕組みを可能にしたところに、ブロックチェーン技術を用いたビットコインの特色があると考えられる。

従前の法的地位の消滅と新たな法的地位の発生という移転の仕組みは、流動性預金口座に対する振込みの法的構造――支払指図により、振込人の預金債権の一部が消滅し、受取人が新たに預金債権を取得する――に類似する(102)。このような仕組みは、法的地位の移転を原因関係の瑕疵から切り離す理解に親和的であるので、決済手段としての利用に適合した法律構成であるということができる。

(b) 移転を求める権利の内容

以上を前提として、あるネットワーク参加者が――例えば、ビットコインの移転と引き換えに商品やサービスを提供するという契約に基づいて――他のネットワーク参加者に対して、ビットコインの移転を求める権利を有する場合に、その権利がいかなる内容のものであるかが問題となる。この場合、債務者であるネットワーク参加者は、債権者であるネットワーク参加者に対して、一定額のビットコインの帰属を変更する義務を負うものと解される。ビットコイン・トランザクションの仕組みを前提とすれば、帰属変更の対象は、特定のデータ（未使用トランザクション・アウトプット）ではなく、一定の額であると考えられるからである。

以上のビットコインの移転に関する説明は、前述した第2の見解（**(1)** ②b(b)）の主張と同様の帰結を導くことになる。

d　無権限者による法的地位の移転

続いて、無権限者による法的地位の移転についてみていこう。前述（**2 (1)**）のように、秘密鍵が漏洩した場合、それを知った者は、その秘密鍵を用いたビットコイン・トランザクションを行うことが可能になる。そして、当該トランザクションが承

(102) 日本銀行決済機構・金融研究所・前掲注(3) 7頁、森田・前掲注(3) 20頁。預金の振込みに関する法律構成の詳細については、森田宏樹「電子マネーの法的構成(3)」NBL619号(1997年) 33頁、36頁注58。もっとも、流動性預金口座においては入金ごとに新たに1つの預金債権が成立するのに対して、ビットコインの場合には、ウォレット内に、移転元とその額を示すデータが未使用トランザクション・アウトプットの形で存在し、移転元を捨象した残高のみの1つのデータにまとめられるわけではない（**2 (3)** 参照）。

認されれば、ビットコインのシステム上、それを覆す仕組みは用意されていない。それゆえ、ビットコイン・ネットワーク上、未使用トランザクション・アウトプットの状態は変更されたままであることになる。

他方、法的な観点からは、法的地位の帰属に対する侵害が問題となる。無権限者によるトランザクションの被害を被ったネットワーク参加者は――債務者の特定の困難という問題は存在するものの――無権限者に対して不法行為に基づく損害賠償請求権を有するほか（民法 709 条）、当該トランザクションによって利益を受けた者に対して不当利得返還請求権を有することになる（民法 703 条、704 条）。問題は不当利得返還請求権の内容である。ビットコイン・トランザクションの仕組み――1 つ又は複数の未使用トランザクション・アウトプットを利用して、新たに別の 1 つ又は複数の未使用トランザクション・アウトプットを作り出すこと――により、元の未使用トランザクション・アウトプットを回復することは不可能になっている。そこで、不当利得返還請求権の内容は、債務者に帰属する一定額のビットコインについて、その法的地位の帰属変更を求めることになると考えられる。他方、債務者が既にビットコインを他者に移転しており、債務者に帰属するビットコインが存在しない場合には、価額の返還を請求すべきものと解される[(103)]。

以上を前提として、議論の対立があるのが、無権限取引の被害者に、物権的返還請求権を認めるか否かである。もっとも、物権的返還請求権を認めるとしても、無権限のビットコイン・トランザクションがなされる以前の状態に未使用トランザクション・アウトプットを回復することはできない。それゆえ、物権的返還請求権の内容は、一定額のビットコインの帰属の変更の請求を意味することになり、その点では、不当利得返還請求権と同様であるといえる。

他方、物権的返還請求権と不当利得返還請求権との違いとして挙げられるのが、ビットコインが第三者に移転された場合における当該第三者に対する請求の可否や、請求権の相手方（債務者）が倒産した場合における取戻権（破産法 62 条など）の成否などである。もっとも、前者については、物権的返還請求権を肯定する見解によっても、第三者が一定の主観的態様（善意・無過失や善意・無重過失）を充たす場合には物権的返還請求権が否定されるものと解されること[(104)]、及び、不当利得返還請求権についても、一定の条件のもとで第三者に対する効力が認められうること[(105)]、に注意

(103) 最判平成 19 年 3 月 8 日民集 61 巻 2 号 479 頁参照（価額を算定する基準時について議論の対立がある）。以上に対して、片岡③・前掲注（3）15-16 頁は、債務者が同種・同量のビットコインを調達する義務を負うものとする。

(104) 金融法委員会・前掲注（3）13 頁。森下・前掲注（3）807 頁も善意取得に言及する。

(105) 最判昭和 49 年 9 月 26 日民集 28 巻 6 号 1243 頁参照。

を要する。

この問題を考えるうえでは、無権限取引の被害者にどの程度の法的保護を与えるのが望ましいのかという実質的判断が要請される。そして、ここで議論の対象とされる無権限取引の被害者が――ビットコイン利用者の多数を占めるネットワーク非参加利用者ではなく――ネットワーク参加者であり、ビットコイン・トランザクションの仕組みや秘密鍵の管理についての専門的知識を期待できることを前提とすれば、被害者の要保護性が類型的に高いとはいえないものと解される[106]。それゆえ、無権限取引の被害者の救済を不当利得返還請求権によるものにとどめるという判断には、合理性があると考えられる。

e　執行・倒産手続上の問題

最後に、執行・倒産手続上の問題についてみておこう。

まず、ビットコインのデータを利用する法的地位は、その帰属主体であるネットワーク参加者の責任財産を構成する。それゆえ、当該法的地位は執行対象適格を有し、それに対する強制執行が許容されることになる。この法的地位は「不動産、船舶、動産及び債権以外の財産権」に該当すると解されるので、その他の財産権に対する強制執行として債権執行の例によることになる（民事執行法 167 条 1 項）。ビットコインの移転はネットワーク参加者相互間に限られるため、換価の方法が制約を受けるものの、そのことによって執行対象適格が否定されるわけではない[107]。

もっとも、実際に強制執行をどのように行うかについては、様々な問題が存在する。まず、ビットコインのシステム上、第三債務者に該当する発行主体が存在しないため、差押えの効力は、差押命令が債務者に送達された時に生ずるものと解される（民事執行法 167 条 3 項）[108]。次に、換価の方法は債権執行の例によるので、取立てを行うことができないビットコインについては、譲渡命令又は売却命令によるべきものとされる（民事執行法 161 条 1 項）[109]。差押債権者がネットワーク参加者である場合には譲渡命令も可能であるが、ネットワーク参加者でない場合には売却命令によるこ

（106）得津②・前掲注（3）27 頁も、このことを示唆する。

（107）中野貞一郎＝下村正明『民事執行法』（青林書院・2016 年）778 頁注 4（民法上の組合の組合持分に対する執行）。

（108）片岡①・前掲注（3）46 頁、高松志直「電子マネーおよび仮想通貨に対する強制執行」金法 2067 号（2017 年）56 頁、石井教文「仮想通貨保有者からの債権回収」金法 2092 号（2018 年）4 頁、後藤＝渡邉（各論）・前掲注（3）107 頁、菅原百合＝髙田和貴「仮想通貨と債権保全・回収に関する実務的考察」NBL1131 号（2018 年）39 頁。

（109）片岡①・前掲注（3）46 頁、高松・前掲注（108）57 頁、石井・前掲注（108）4 頁、菅野＝髙田・前掲注（108）39-40 頁。

とになる。もっとも、譲渡命令・売却命令を実行するには、差押債務者から秘密鍵についての情報提供を受ける必要があり、差押債務者が協力を拒む場合には、これらの方法によって換価を行うことが困難である。そこで協力を拒む差押債務者に対しては、間接強制（民事執行法 172 条）によらざるをえないが、実効性に欠ける場合もあると考えられる[110]。

以上の執行手続の問題は、既に電子マネーについて論じられてきたところと重なる[111]。もっとも、電子マネーについては、「発行者があり、その発行者が第三債務者となるから、その協力が得られれば強制執行の実効性を確保できる余地[112]」があり、またそもそも「強制執行の可能性等も考慮に入れて、電子マネーの商品性自体を工夫していく必要[113]」が指摘されていた[114]。これに対して、発行者の存在しないビットコインについては、執行手続に関する問題が、より深刻な形で現れるのである[115]。

以上の議論は、倒産手続にも妥当する。ネットワーク参加者に対する倒産手続が開始した場合、ビットコインは倒産財団を構成することになる。ただしこの場合にも、破産管財人などが換価を行うには、秘密鍵の提供など倒産者の協力が必要になるのである。

このように考えると、現在のビットコインの仕組みは、執行・倒産手続の実効性を損なうものとなっている。私人の合意によって執行・倒産手続を事実上回避できる財産が作り出されることを可及的に防止することが、法的に重視される価値であるとすれば、現在のビットコインに対する重大な懸念の 1 つは、以上にみた執行・倒産手続上の問題であると考えられるのである。

② ネットワーク非参加利用者の法的地位

ａ ネットワーク参加者との契約関係

続いて、ネットワーク非参加利用者の法的地位の検討に移ろう。ネットワーク非参加利用者は、ネットワーク参加者（仮想通貨交換業者など）を介してビットコインの

---

(110) 片岡①・前掲注（3）46-47 頁、高松・前掲注（108）57 頁、石井・前掲注（108）4 頁、後藤＝渡邉（各論）・前掲注（3）107 頁、菅野＝髙田・前掲注（108）40 頁、金融法委員会・前掲注（3）21 頁、本多（2・完）・前掲注（3）1220-1221 頁。

(111) 電子マネーに対する強制執行の問題について、岩原紳作『電子決済と法』（有斐閣・2003 年）502-505 頁。

(112) 片岡①・前掲注（49）46 頁。

(113) 岩原・前掲注（111）505 頁。

(114) このほか、電子マネーに対する具体的な執行方法については、高松・前掲注（108)52-56 頁。

(115) 中野＝下村・前掲注（107）778 頁注 6 は「デジタル財執行に適した手続整備を早急かつ不断に追及しなければならない」とする。

取引を行うのであり、両者の間には契約関係が存在するものと考えられる。この場合、ビットコインに関する法的地位の帰属主体は、ネットワーク参加者であって、ネットワーク非参加利用者ではないと解される。ネットワーク非参加利用者は、ネットワーク参加者に対する契約上の債権――ネットワーク参加者に対してビットコインの取引（法的地位の帰属の変更）に関する指図を行う権利など――を有するのである。

ネットワーク非参加利用者とネットワーク参加者の間の法律関係は、契約によって規律されることになる。それゆえ、ビットコインの取引について生じうる問題――例えば、無権限者による指図に従ってビットコインの取引が行われた場合における損失の負担――について、予め合意をしておくことが考えられる。そのような合意の有効性は、消費者契約法を含む契約法の規律に従って判断されることになる。

b　執行・倒産手続上の問題

（a）ネットワーク非参加利用者に対する執行手続・倒産手続

次に、ネットワーク非参加利用者の法的地位に関する執行・倒産手続上の問題についてみていこう。この点については、ネットワーク非参加利用者に対する執行・倒産手続と、ネットワーク参加者に対する執行・倒産手続を区別して論じる必要がある。

まず、ネットワーク非参加利用者がネットワーク参加者に対して有する契約上の債権は、その者の責任財産を構成する。それゆえ、ネットワーク非参加利用者の債権者は当該債権に対して執行を行うことができる[116]。この場合、差押えの効力は第三者債務者であるネットワーク参加者への送達の時に生じる（民事執行法145条4項）。換価の方法は、譲渡命令・売却命令（民事執行法161条1項）によるものと解される[117]。

また、ネットワーク非参加利用者に対して倒産手続が開始した場合には、ネットワーク非参加利用者のネットワーク参加者に対する債権が、倒産財団を構成する。そ

（116）菅野＝髙田・前掲注（108）40頁。債権執行の実例を紹介するものとして、藤井裕子「仮想通貨に関する返還請求権の債権差押え」金法2079号（2017年）7頁。なお、高松・前掲注（108）57頁は、仮想通貨交換業者の顧客が債務者である場合を念頭に置いて、「仮想通貨自体に対する強制執行とは別に、仮想通貨交換業者に対する請求権を対象とした差押えが実務上有益な選択肢になる」とする。しかし、仮想通貨交換業者の顧客に仮想通貨が帰属している（それゆえ、強制執行の対象となる）といえるかには疑問がある。

（117）高松・前掲注（108）58頁。もっとも、今後の執行方法の在り方を考えるうえでは、執行官がノードを保有する（ネットワーク参加者となる）ことで、第三債務者に対し、執行官へのビットコインの移転を求めるという手法も検討に値するように思われる（高松・前掲注（108）58頁注44参照）。

れゆえ、例えば、破産管財人は当該債権を行使してビットコインを処分し、配当の原資を確保することができる。

ネットワーク参加者である仮想通貨交換業者については、顧客（ネットワーク非参加利用者）に対する執行・倒産手続の開始を念頭に置いて、以上のような法的取扱いに対応できるシステムを構築しておくが望ましいと考えられる[(118)]。

（b）ネットワーク参加者に対する執行手続・倒産手続

次に、ネットワーク参加者に対して執行・倒産手続が開始した場合については、前述のように、ビットコインに関する法的地位は、その帰属主体であるネットワーク参加者の責任財産に属するのが原則である。しかし、ネットワーク非参加利用者のために、ネットワーク参加者が法的地位の帰属主体となる場合には、そのことの法的評価が問題となる。ビットコインの取引について、専門的知識を有するわけでない多数の利用者を保護するという観点からは、この問題が重要な意義を持つことになる[(119)]。

この点について、ネットワーク参加者を受託者、ネットワーク非参加利用者を受益者とする信託という法律構成を用いることにより、信託財産であるビットコインに関する法的地位がネットワーク参加者（受託者）の責任財産から除外されるという法的効果を導くことが考えられる[(120)]。その場合、ネットワーク参加者の債権者がビットコインに関する法的地位を差し押さえても、ネットワーク参加者又はネットワーク非参加利用者が第三者異議の訴えを提起することができる（信託法 23 条 5 項、民事執行法 38 条）。また、ネットワーク参加者に対する倒産手続が開始した場合も、ビットコインに関する法的地位は破産財団や再生債務者財産などに含まれないことになる（信託法 25 条 1 項、4 項）。ビットコインは、新たに受託者となるネットワーク参加者に移転され、そのもとで信託が継続するのである（信託法 60 条 4 項、75 条 1 項）。

もっとも、このような法律構成を採用する前提として、問題となるビットコインが信託財産としての特定性・独立性を有する必要がある。この点で、ネットワーク参加者が、自己の取引に用いるのとは別のノードを利用して、ネットワーク非参加利用者

---

(118) 執行手続における仮想通貨交換業者の対応について、藤井・前掲注（116）8 頁。また仮想通貨交換業者の実情に対する批判として、石井・前掲注（108）5 頁。

(119) 得津②・前掲注（3）27 頁も、「消費者保護を論じるのであれば、顧客が取引所に対して有するアカウントの法的保護を検討すべきである」と指摘する。

(120) 仮想通貨の法的性質の理解の仕方にかかわらず、ビットコインの信託を肯定する見解が有力化している（田中＝遠藤（下）・前掲注（3）76-77 頁、武内・前掲注（3）16 頁、西村あさひ法律事務所編・前掲注（3）855-856 頁〔芝章浩〕、後藤＝渡邉（各論）・前掲注（3）106 頁、金融法委員会・前掲注（3）19 頁、本多（2・完）・前掲注（3）1203 頁、芝②・前掲注（3）54 頁）。ただし、仮想通貨交換業者が業として信託の引受けを行う場合には、信託業法の適用が問題となる。

のための取引をしていることは、信託という性質決定をするのに有利に働くと考えることができる(121)。

4　おわりに

技術の進展とともに、社会においてプログラム・コードが規定する領域は、今後も拡大していくことが予想される。その中で、法律家には、プログラム・コードの内容を理解し、それに適合する法律構成を検討することが求められるとともに、プログラム・コードの内容を法の観点から批判的に評価し、爾後のプログラム・コードの在り方に影響を与える議論を蓄積することが期待されるように思われる。

仮想通貨の法的性質をめぐるわが国の議論状況は、以上のような法律家の役割を考えるうえで、格好の題材であるといえる。この題材の検討を通じて、本稿が、法とプログラム・コードをめぐる議論の深化の一助となれば幸いである。

【追記】 脱稿後、道垣内弘人「仮想通貨の法的性質――担保物としての適格性」道垣内弘人ほか編『近江幸治先生古稀記念 社会の発展と民法学 上巻』（成文堂・2019年）489頁に接した。同論文は、仮想通貨の法的性質について、「《自分が他者から承認されている保有単位数を、他の参加者に移転することができる権利》」（494頁）であると解し、「このような権利は、ネットワーク上の合意によって成立していると考えてよいであろう」（495頁）とする。また、「アドレス」を保有する仮想通貨の交換業者と保有しない顧客を区別し、交換業者が上述の権利を有するのに対し、顧客は通常「交換業者に対する債権を有しているにとどまる」（496頁）とする。以上の理解は、本稿の立場と親和的であるように思われる。

他方、同論文は、例外的状況のもとで、顧客が、「《自分が他者から承認されている保有単位数を、他の参加者に移転することができる権利》を直接的・排他的に支配する権利」を有すると考える余地があるとし、その場合には「顧客の有する権利を物権的に捉えることができよう」（497頁）とする。合意に基づく権利が「アドレス」の保有者（交換業者）に帰属することを前提として、当該権利を「直接的・排他的に支配する権利」が顧客に帰属するものとし、それを「物権的」と表現するところに、同論文の特色があるといえる。

---

(121) なお、冒頭で紹介したMt. Gox社は、この種の分別管理を行っていなかったのであり、東京地判平成27年8月5日（前掲注（4））が顧客の取戻権を否定したことは（前掲注（51）参照）、結論として妥当であったと考えられる。