

## 仮想通貨と通貨をめぐる 法規制の一試論（上）<sup>1</sup>

弁護士  
長野 聡

現在仮想通貨と呼ばれている多様なものを実態に即して分類し、既存の国家（中央銀行）通貨（現金＝銀行券＋貨幣。以下「国家通貨」という）、支払手段（預金等）、金融商品（株式、債券等）と比べて、制度（以下、規制、私法上の扱い等を含む）上、同等に扱うべきか否かの包括的検討が必要である。分類の基点は、国家通貨と同様に通貨として機能しうる仮想通貨は何かである。

通貨の条件は価値、流通の安定への信用であり、現時点で満たすのは、P2P内でメンバーが価値維持行動をすとの信用に依拠した仮想通貨（以下「P2P内信用仮想通貨」という）と発行体または管理者への信用に依拠した仮想通貨（以下「主体型仮想通貨」という）に限られる。P2P内信用仮想通貨は現実には仮想通貨の仕組みに関与できる専門家間には存在せず、将来は地域通貨等に可能性がある。主体型仮想通貨は銀行等信用ある主体や見合い資産のある信託の仕組みにより発行管理される可能性がある。後者は国家通貨同様に規律し、通貨の条件を満たさない仮想通貨と呼ばれるものは実態に合わせて円の支払手段や金融商品と同等の制度に服すべきである。

### 1 問題意識

仮想通貨の現実の展開は、社会のほかの先端分野と同様に、速すぎてかつ安定していない。そのため無理からぬ面は多分にあるが、以下のように現実の展開に制度が追いついていない。

#### (1) この1年ほどの現実の展開

##### a 仮想通貨の種類増加

フォーク（ブロックチェーンの分岐）、既存

プラットフォーム（イーサリアムなど）の利用などの方法で新しい通貨（アルトコイン）が多く発行され（仮想通貨だけで2000とも3000ともいわれているほか、ICOも入れると数百万種ともいわれている）、規制のゆるい地域（タックスヘイブン）などの交換所で取引され、簡単な英語ができれば誰でもインターネットで取引できる。注目すべきは数の増加だけでなく、国家（中央銀行）への信用に依拠せず、価値保有や移転の正当性をP2Pメンバー内の誰でも平等に参加できる競争によるマイニングにより担

1 学習院大学・神田秀樹教授、中央大学・黒田巖元教授、早稲田大学・岩村充教授、東京大学・森田宏樹教授、東京国際大学・本多正樹教授、京都大学・岩下直行教授、慶應義塾大学・斉藤賢爾講師、藤井典子講師、日本銀行金融研究所の鹿島みかり氏、千葉誠氏、橋本崇氏、平良耕作氏、清藤武暢氏、森田泰子氏からは貴重なアドバイスをいただいたことを感謝申し上げます。なお、文中の意見にわたる部分は筆者の個人的意見であり、またありうべき誤りもすべて筆者の責任であることをお断わりする。

2 Peer to Peerとは同等の立場にある仲間内のこと。本稿では、P2P内信用仮想通貨という用語は、通貨の信用が成り立つという観点から、価値維持行動を取るという意味での信用関係にある仲間内という拡張した含意で使っており、P2Pという技術用語に、さらに信用関係がある場合を想定した用語として使用している。日本の講、中国の幣のイメージである。

## 目次

### 1 問題意識

- (1) この1年ほどの現実の展開
- (2) 仮想通貨の実態に即した分類と国家通貨（現金）との関係整理の難しさとの不可欠性
- (3) 仮想通貨分類の基準と検討の視点

### 2 実態に即した仮想通貨の分類

- (1) 前提としての通貨（現金 = 日本銀行券 + 貨幣）の条件
- (2) 仮想通貨の分類（以上、本号）

### 3 仮想通貨（P2P内信用仮想通貨、主体型仮想通貨に限る）に係る制度の在り方

- (1) 発行・流通に係る規制

- (2) 私法上の扱い

### 4 仮想通貨建て支払手段・金融商品、決済に使われない仮想通貨に係る制度

- (1) 仮想通貨建ての決済手段、金融商品の規律

- (2) 決済に使われない仮想通貨に係る制度

- (3) 金融商品取引法上の投資対象と位置付けられた仮想通貨を扱う交換所の業務規制

（以上、次号（2093号）掲載予定）

保しようとした仮想通貨から、価値保有や移転の正当性の証明をマイニングではなく、競争条件を既存保有者等に有利にして証明させる仮想通貨が出現していることである。こうした仮想通貨は、ブロックチェーン技術を利用した仮想通貨の価値移転に加えて、商流その他の情報の流通・移転も行えるようなプラットフォームを提供しており、管理者やそれに準じるコアメンバーがいる点に特色がある。こうした動きは、価値保有や移転の正当性担保の方法において多様な通貨が出てきていると評価できる。

さらに銀行等法人も仮想通貨を発行することを表明しており、発行体や仕組みの管理者（信頼できる第三者）が明確に存在して、保有や移転にも責任を負う仮想通貨も検討されている。

また、デジタルマネーを発行した中央銀行（ベネズエラのPetro等）があるほか、世界のいくつかの中央銀行も発行を検討すると表明している。

#### b 交換所での取引量増大によるP2P内信用仮想通貨という理想の崩壊

サトシ・ナカモトの原論文やその後の黎明期のブロックチェーン技術を利用してP2P内のマイニングにより確率的に価値保有や移転の正当性を担保する仮想通貨の構想は、ブロックチェーンの数の増加とマイニングコスト（コンピューター能力と電気代支払能力）の増加によるマイナーの寡占化、交換所を利用する一般利用者の増大によって崩れた状態にある。

一般利用者は秘密鍵の自己管理の面倒を避けるため交換所に秘密鍵を含め管理を委託して仮想通貨の交換を他の一般利用者で行ったり<sup>3</sup>、交換所との間で国家通貨や他の仮想通貨との交換をしたりするようになっている（このことは後述のように面倒なことはしないのが、一般利用者という意味で仮想通貨の未来を暗示していると思われる）。もはや、信用関係があるP2Pといえるのは、開発者、マイナー、その他フルノード<sup>4</sup>を自分で持って管理する特定の少数参加者に限られ、交換所に仮想通貨を預けて（秘

3 利用者と交換所の関係には、利用者が秘密鍵を交換所に完全に預けて（利用者自身が秘密鍵を知らないケースが大半ともいわれている）、交換所を通じなければ交換所はもちろん、他の利用者との取引できないタイプ、利用者と交換所が秘密鍵をともに使えるタイプ、利用者が秘密鍵を自己管理し取引アプリだけを利用するタイプがあるが、利用者のほとんどは最初のタイプといわれている。

4 ブロックチェーンすべてをダウンロード、検証し、不正なブロックがないかを監視して、他のノードや通常の利用者にブロックチェーン情報を伝達する役目を持つコンピューターのことである。担い手はボランティアが多く、減少している。

密鍵も預けるケースが多い) いる一般利用者もはや信用関係あるP2Pの中に入っていない。このことは、仮想通貨が通貨として使われる条件である信用関係がP2P内の信用を担保する仕組みにあるという理想の崩壊を意味している。もとより主体型仮想通貨はP2P内の信用を担保する仕組みではなく、その仕組みや仮想通貨の見合い資産(ある場合)を維持する銀行等の信用力に通貨の根拠があるので、ブロックチェーンを使っているとしてもその原理は全く異なる。

#### c 取引量著増・価格乱高下・投機的利用拡大・犯罪の発生

仮想通貨の世界での取引量は2016年に1日当たり100億円から400億円に拡大し、2017年には最大3兆円にもなった。太宗は証拠金取引(レバレッジ取引)とされ、価格は取引量が最大のビットコインで1日25%程度も変化した例があり安定しない。2018年3月末時点では、時価総額は27兆4339億円のうちビットコインが最大で45.2%を占め、その取引の6割近くが対円交換である(金融庁「仮想通貨交換業等に関する研究会第1回」資料3より)。このように日本の交換所は世界の仮想通貨取引の最大の場になっている。個人外為取引の低調は、投資家が外為から仮想通貨にシフトしていることが原因ともいわれる。

一方でMt. Goxやコインチェックでは仮想通貨の盗難が起き、匿名性の高い仮想通貨がマネーロンダリング(以下「マネロン」という)に利用されている疑いも強くなっている。本来ブロックチェーンはマイナーや開発者が結束すれば、すべての取引記録は普遍的にノードに残るので、ノードとその主体との紐付けはともかく、ノードの記録を匿名には当然にはできないはずだが、コインチェックにおけるNEMの秘密鍵盗難では、結局NEM財団にも、ましてマイナーにも盗難を追いかける明確なインセ

ンティブがなく、ダークサイトに拡散した2次取引の追跡は警察組織がマイナーと同等の能力を持たない限り、ホワイトハッカーだけでは犯人は捕まりそうもない。

#### d 秘密鍵管理技術の進展と量子コンピューターの開発目処

ブロックチェーンによる情報は、秘密鍵を盗まれば排他的な管理(法的には厳密な定義が必要であろうが、ここでは米国のcontrolと仮置きしておく)は不可能になる。このため秘密鍵の管理やそれを読み取られないための工夫はいろいろな技術を組み合わせることで無限に考えられ、現にそれが試みられているよううかがえる。複数名署名(マルチシグ)、第三者機関(認証機関)の関与、さらには主体型仮想通貨の場合には、マイナーも指定されることになり、ブロックチェーンを使っている情報移転は、中央機関(信頼できる第三者、銀行やその関連主体)が、真正性を担保する預金や債券(振替決済)の仕組みに類似したものになる。そうしたことは、マネロンや犯罪には使わないという意味において、P2P内の信用を担保する仕組みに依拠した仮想通貨の構想からは大きく離れた通貨を作ることになる。

さらに、次元の違う技術変化としては、米国は現在の公開鍵暗号を短時間で破りうる量子コンピューターが12年程度で完成すると見込み、2026年に耐量子コンピューター暗号へ移行する計画を示している。共通鍵でも対策が必要であるので<sup>5</sup>公開鍵ではより対策が必要になる等、仮想通貨の流通にはまだまだ技術面における不確定要素がある。

#### (2) 仮想通貨の実態に即した分類と国家通貨(現金)との関係整理の難しさとの不可欠性

前記(1)bの仮想通貨の保有と取引の容易化が、仮想通貨の多種発行(前記(1)aおよびc)、P2Pに参加しない購入者の著増、そして仮想

5 「米国連邦政府は、現在主流のRSA暗号を数時間で解読する量子コンピューターが2030年までに実現する(筆者注:可能性はある)との見解を示したうえで、2022年頃までに耐量子計算機暗号の政府調達基準を策定し、現在使用している公開鍵暗号を2026年頃までに耐量子計算機暗号へ移行する計画を示している」(清藤武暢=四方順司「量子コンピューターが共通鍵暗号の安全性に与える影響」日本銀行金融研究所Discussion Paper Series 2018-J-2・1頁)。

通貨の投機対象化を生んでいる。仮想通貨という名称にかかわらずその実態は、価値の安定が成立条件である通貨と乖離したものが多数存在している。このため仮想通貨の制度を検討するに際しては、一括扱いではなく、その実態に応じて分類整理すること<sup>6</sup>が不可欠である<sup>7</sup>。

分類にあたっては、通貨が国家通貨に収斂してきた歴史<sup>8</sup>にかんがみると、現状、仮想通貨と呼ばれるものの中に「国家通貨と差がなく日常の決済に利用できるという意味」での通貨性を持つものがあるかを基点とするのが便宜かつ必要である。

便宜な理由は、通貨性のある仮想通貨を限定できれば、仮想通貨建ての決済手段や金融商品（株式、債券など）が存在しうることになり、対応する国家通貨（円）、円の決済手段、円の金融商品にかかる制度の当てはめの適否を考えるのに見通しがつけやすい。

必要な理由は、通貨が受け入れられる条件である信用は、そもそも使われれば使われるほど信用されるという経済学というネットワーク外部性（externality）があり、加えてそのための制度がまた一段と通貨としての信用を高めるといふ二重のネットワーク外部性があるためである。これが、通貨が制度的担保のある国家通貨に収斂してきた一つの理由と考えられる。

本稿は、国家の信用に依存しない通貨の多様性を、利用者の利便性と通貨制度の安定性の観

点から支持する立場を採るが、歴史的には制度的担保のない通貨は大きな混乱を利用者に生む結果しかもたらしていない。仮想通貨の問題を国家通貨と関係なく論じることは、それが通貨の問題である以上不十分である。通貨制度全体<sup>9</sup>の中で、仮想通貨の制度上の扱いの不透明さを払拭し、社会に適合させてゆくことが、使い勝手が良い仮想通貨の利用拡大を促すイノベーションにもつながる一方で、セキュリティや盗難などの病理的な出来事における混乱を最小限にとどめることにもつながりうる。

例えば、日本の歴史的にも金や銀も採掘したままで当然に通貨であったわけではなく江戸幕府が加工、発行し、制度と相まって通貨として機能した<sup>10</sup>。日本では、最初は制度作りが後手に回り実態が自由放任に先行し、その後、病理的な出来事が起きると厳しい法規制が置かれイノベーションを阻害する例も多い<sup>11</sup>。

もっともこの分類は本質的な困難さを伴う。それは、通貨は利用者群がそれを通貨だと信用して受け入れれば、何でも通貨になりうるからである。通貨と金融商品は、使われる取引局面ではどちらかは明らかだが、全体としてみると使う人（法人）、使われる目的でどちらにもなりうる。例えばドル紙幣は、日本商社が貿易決済に使うときは通貨だが、資金運用で買うなら金融商品である。昭和初期に日本の大銀行が円売りをした時には、円も通貨ではなく、金融商

6 金融庁の機能別・横断的な金融規制の整備（金融審議会金融制度スタディ・グループ）、仮想通貨交換業等に関する研究会もそうした問題意識によっていると思われる。

7 資金決済に関する法律（以下「資金決済法」という）が仮想通貨を定義しているが、これも仮想通貨が多様化する前にビットコインなどを念頭にマネロン抑止の観点から立法されたもので、その定義によりすべて制度問題が解決したとはもはやいえない。金融商品も含みうる定義は、広すぎて適切と思われない。

8 江戸幕府は金、銀、銭貨の鑄造発行を直轄していたが、紙幣としての山田羽書（注12参照）や藩札について最初は放任していたが、濫発による信用不安やインフレを機に関与を強め、事実上発行を管理し干渉した。日本銀行は、国立銀行の紙幣濫発によるインフレ收拾のために設立された。その後、国家通貨だけでは経済発展に追いつかないため信用創造と相まって長い時間かかって銀行預金が通貨と同視されるようになった。

9 仮想通貨と国家通貨を含む通貨制度全体は財務省の所掌である（財務省設置法4条30号）。

10 江戸時代の金銀複本位制も金や銀が当然に通貨として保有、流通したわけではなく、江戸幕府は金銀貨の製造過程や品質、その保証（刻印、後藤家のサインなど）に関与している。

11 大正11年に不良な信託会社を整理するための信託業法が制定されたが、免許付与に厳しい運用がなされ、戦後には信託業法による信託会社はすべて消滅し、金融機関の信託業務の兼営等に関する法律による信託銀行以外の信託業は、平成16年の信託業法改正まで認められなかった。信託は濫用の歴史といわれる一方で、超高齢社会における需要不足に十分対応できない事態を招いている。仮想通貨もマネロンねらいでの利用、交換業者を含めた杜撰な管理など病理的なケースが目につくが、これを全面禁止してしまうとイノベーションを阻害しかねない。

品になった。現在では国内で円の価値を日常決済で疑う人はいないが、世界では国家通貨を信用していない国民が大半ともいえる。

しかしだからといって、現在の日本で全部の仮想通貨が通貨として信用されるだろうか。明らかに通貨でないものは通貨として遇することはできないので、自明な程度分類はやはり不可欠であろう。大事なことは、ある程度確からしい技術進歩を踏まえて、当面の規制やルールなどの制度を作り、透明性を確保しつつ、事態の推移によってはそのルール、制度を柔軟に変更していくことである。仮想通貨をめぐる上記の激しい変化は、預金通貨が通貨となる過程で当事者や市場、裁判所がルールを作ったという悠長さを、経済的影響、国際競争、信用秩序維持の観点から許すだろうか。

もちろん、制度は必ずしも成文法によるとは限らない。歴史的にみても慣習や利用者間の信用関係に基づく通貨もありえた<sup>12</sup>のであり、とくに技術進歩が見通しにくい場合には、成文法でなく、契約や慣習による制度作りがふさわしいということもありうる。しかし、繰り返しになるが、それは仮想通貨の実態と国家通貨との関係を整理せずともよいということを意味しない。通貨全体の中で仮想通貨の問題の整理をすることが、交換所団体の自主規制に軸を与え、ICOや銀行またはその関連会社による仮想通貨の発行または帳簿管理にも明確な制度上の位置付けを与えることに資すると考える。

### (3) 仮想通貨分類の基準と検討の視点

現状、仮想通貨と呼ばれるものの中に「国家通貨と差がなく日常の決済に利用できるという意味」での通貨性を持てるものがあるかを判断する基準は、当該仮想通貨が通貨として利用者に受け入れられるための信用が具体的に成り立つか否かである。歴史的には、信用は、顔のみえる範囲での仲間内（P2P）の人間的な信頼・信用関係または信頼できる第三者である国家（鎌倉・室町時代は宋・明など）や地域政府（江戸時代は藩）への信用であった。同様に現状の仮想通貨の中に、P2P内の信用を担保する仕組みが成り立つ<sup>13</sup>P2P内信用仮想通貨があるか<sup>14</sup>、信用できる発行体や帳簿など仕組み全体を管理する管理者が存在する主体型仮想通貨があるか、が問題になる。

ここで発行体と管理者は、信用の源泉という意味であり、何らかの法的責任を負うことを必ずしも意味しない。不換紙幣である現行日本銀行券の保有者が日本銀行に対していかなる権利を持つかは法的な議論はありうるが、日本銀行自身の政策業務への信用（金融政策に限らず金融システムの安定や決済業務の安定的運行、ひいては組織への信用も含む）や日本国に対する信用、通貨の安定流通の仕組み全体が信用の源泉であり、ここでの発行体や管理者はそうした仕組みを担う担い手という意味である。そうした担い手への信用が、通貨として機能するための源泉であり、担い手の権限と責任を制度とし

12 江戸幕府は、最初の紙幣といわれる山田羽書（江戸時代を通じ伊勢の神職らの仲間が発行・流通した）に対して、当初、発行を容認、監視しつつも介入しなかったが、元文の金銀改鑄を機に兌換請求が増大し取付けが発生して以降、発行量、製造手法を山田奉行が監督した（藤井典子「幕府による山田羽書の製造管理」金融研究31巻1号53頁）。一方、商人などが私的に発行した摂津・平野郷町で流通した札は、江戸幕府は関与せず、限られた地域・仲間内で長く流通したほか、東海道の宿場では、整備事業の人手労賃の支払に一種の通貨代用証書を渡し、後日、正貨（銭）に引き換えた。信用する仲間内での支払に用いる通貨は偽造対抗力が強い必要がない（製造面の意匠も簡素）が、山田羽書のように伊勢地方から周辺の大名領（紀州・津幡等）まで広域流通した札では、江戸幕府が準備資産積立てを含め制度的関与を強めている（本注は、慶應義塾大学・藤井典子講師から教示を受けた）。

13 サトシ・ナカモトの原点（ハイエクの貨幣発行自由化論にも、お金の本質論にも立ち返ることになる）は、国家通貨に依存しないというP2P内の通貨を作ることであった。

14 一般利用者は交換所に仮想通貨を預けて、交換所と取引（販売所）、または交換所が仲介して他の保有者と取引（取引所）することが多い。ブロックチェーン技術とマイニングによって取引の真正性を担保するP2Pの仲間内の信用関係が、取引の相手方との間にあるわけではない。一方、通貨としての利用面でも、実際にビットコインのように小売決済で使われている仮想通貨が出てきているが、国家通貨に比べて小額でレバレッジ取引がほとんどであるため、国家通貨同様の機能を持っていない。

【図表1】通貨、決済手段、金融商品の理想型の分類

通貨建て種類	通貨（現金）	決済手段	金融商品
円建て	日本銀行券、貨幣	金融機関預金、手形・小切手、クレジットカード	株式、債券、デリバティブズ取引等
ドル建て	ドル札、ドルコイン	同上	（自ら決済に使わない外国通貨建て*1） 現金、預金（すべての通貨建て） 株式、債券、デリバティブズ取引等
仮想通貨建て	（P2P内の信用に基づく） P2P内信用仮想通貨*1  （発行体または管理者の信用に基づく） 主体型仮想通貨*2	（P2P内信用仮想通貨または主体型仮想通貨建て） 同上	（自ら決済に使わない仮想通貨建て*1） 現金、預金（すべての通貨建て） 株式、債券、デリバティブズ取引等*3

詐欺的なICO

※現金相当仮想通貨（後記3参照）

（一般的に仮想通貨と呼ばれているもの）

- \*1 ある県のA市中心に通用するAコインを例として考える。地元金融機関がAコイン建ての預金口座の開設に応じ手形を決済手段として発行し、地元企業が給料を従業員にAコインで払い、従業員はAコイン建ての給料債権を持ち、当該企業がAコイン建ての株式や社債を発行するイメージである。このとき円とAコインを通貨（国家通貨+仮想通貨）として生活する従業員とその家族にとっては各種通貨（円、ドル、Aコイン、ビットコイン）建て株式や債券はもとより、円とAコイン以外の通貨（ビットコインやドル）や当該通貨建ての預金も金融商品になる（ドル預金が国内居住者にとって（経済的には）金融商品であるのと同じである）。
- \*2 MUFGコインなど。
- \*3 IPOに準じるICOによるコインは、投資的なものは法的には株式、持分権、集団投資スキームに該当する。また、資金調達により興された事業によるサービスの割引利用券であれば、サービス割引利用債権と考えられる。

て作ることが必要になる。以下、後記2で仮想通貨を分類して、国家通貨と同等に扱うべきものが何かを特定し、そうした仮想通貨に係る制度を後記3で検討する。

仮想通貨の分類検討（【図表1】）にあたっては、第1に制度を整えることが価値の安定につながるという歴史的事実を踏まえた通貨と制度の相互性・同時決定性、第2にP2P内信用仮想通貨等の通貨の多様性が生まれることを経済厚生向上に資するものとして肯定する立場からイノベーションを阻害しないこと、第3にインターネットという無国籍な空間での事象であるため国家内の法秩序だけでは十分でないこと、の3点を意識する。国際的には日本が今や仮想通貨流通のメッカであり、ICOを日本で、居住者向けに行いたいとの相談が著増していることからみても、対応は喫緊の要請であり、また日本が世界をリードするよい機会と考える。

注意すべきは仮想通貨建ての預金は現在存在しないが、利用者が秘密鍵も含めて（投資商品ではなく）現金同等の仮想通貨を交換所に預け、現在のように明確な契約なく寄託している

状況がさらに進み、消費寄託契約を結べば、交換所は仮想通貨建て決済性預金を受け入れている銀行の機能を果たしうることである。こうなると、現金から預金通貨へ支払手段が拡張した歴史のように仮想通貨から仮想通貨建て預金へ支払手段が拡張することになる。その場合、当該預金の払出しと、前払式証券と為替による資金移転との区別は難しく、この点の資金決済法の見直しが必要である。

## 2 実態に即した仮想通貨の分類

現在仮想通貨と呼ばれているものを分類する前提（後記(2)）として、通貨が通貨として受け入れられ、実際に使われるための条件を検討する（後記(1)）。その条件を仮想通貨と呼ばれているものが満たしていれば国家通貨に準じて制度を作ることが考えられるほか、条件を満たさないならば実態に即して決済手段（預金など）や金融商品（株式、債券、集団投資スキームなど）に準じて制度を構築することが考えられる（後記3）。

(1) 前提としての通貨<sup>15</sup>（現金＝日本銀行券＋貨幣）の条件

通貨がいつでもどこでも誰にでも決済に使えるという意味で「通貨」として機能するためには、通貨の価値が安定することが必要であることは歴史的、経済的に明らかである。その価値の安定は、利用者が、価値が安定すると信用することによりもたらされる。その信用は、歴史的にみてもいくつかの条件が揃う必要がある。大きくは保有や移転のためのコストが小さい<sup>16</sup>ことのほかに、以下の二つの条件が必要になる。

A 通貨の保有や移転が排他的な支配（コントロール）のもとに行うことができ、かつ決済にファイナリティ（一度支払をすれば、支払以外の原因関係によりその支払が無効になったり、取り消されたりしない）があること。このうち排他的支配は、A-①使用されている物理的技術（金属、紙、電気信号など）に負う部分が大きく、物質的に安定している、偽造・複製されにくい、二重譲渡が困難、などを意味している。ファイナリティはA-②法制度（私法上の位置付け、それを実現できる裁判、警察制度など）のほか、発行体や管理者が、無効宣言などをしないという信用によって（裏切った例としては、日本の戦後の新円切替えなど）。

B 信用の源泉である発行体や管理者が権力、権威として安定して存続すると見込まれ、かつ通貨の経済的価値が安定していること（これらの点で、発行体または管理者がある場合にはそれらが信用できること）。このうち主体としての安定は、B-①権力

や権威を損なわないで存続することによって、経済的な価値が安定していることは、B-②発行見合い資産の価値が安定していること、またはB-③（金属貨幣のように）見合い資産がない場合には希少性を通じて価値が安定していることを指す。また見合い資産の有無にかかわらず通貨の流通実態の裏側にある経済実態と合わない大量発行により価値下落がないことも、経済的な価値の安定の要素である。

現在の日本銀行券は、コントロールは紙（A-①）という物理的なモノの占有、ファイナリティは占有＝所有という慣行（最二小判昭39.1.24判時365号26頁・最二小判昭29.11.5刑集8巻11号1675頁、A-②）により確保され、ほかにも治安の良さ（人心、民刑事法制、裁判、警察制度など）などによりAの条件を満たしている。とくに、政府が裁判やその強制執行も含め通貨取引に係る法制度やそのほかの制度を安定的に構築運用することについて信用できることが、通貨利用者が日常意識しているか否かはともかく大きな意義がある。本稿はこうした制度作り（A-②）を検討するものである。なお、Bの条件は日本銀行の業務全般（金融政策（B-②）、B-③）だけではなく、金融システムの安定や発券銀行、銀行の銀行、政府の銀行としての業務全般（B-①）ひいては日本経済の安定性や日本国の持続性への信用こそが、通貨が通貨として機能する源泉である。

とくにBの条件については、発行体や管理者がないP2P内信用仮想通貨では、利用者が信用する対象は、発行、保有・移転の正当性を担保するルールを決め、それを守るというP2P内の仲間への信用という点が目新しい（ただし、こうした通貨が歴史的になかったわけでは

15 現在では、通貨は国家通貨と預金通貨しかない。ここでは国家通貨との比較で考える。

16 日本銀行券や貨幣の重さはコストになる一方、その流通を支える仕組み（金融機関、流通運送業者、自動販売機）はコストを低下させる。利用者にとっては仮想通貨の保有・移転コストは小さくなっておりこの条件を満たす。ただし、そのコストはマイナーがマイニングにかかる電気代やコンピューター設備代で払っており、その報酬は、仮想通貨の流通分、国家通貨が使われなくなることによる国家のシニョリッジ（通貨発行益）の減少という形で国家から奪取されている筋合いにある。この一種の国家（中央銀行）の利益減が利用者にチャージされればコストが安いかは何ともいえないが、利用者が自ら直接負担するコストは低く、通貨の条件は満たされると考え、本稿では問題にしない。

ない。注12参照)。

本稿は、仮想通貨と呼ばれているものが通貨として使われる条件として法制度の仕組み(A-②)を検討するものであるが、発行体や管理者がないP2P内信用仮想通貨では、P2P内で価値を安定させ、価値を維持する行為を仲間がすることに信用があること、主体型仮想通貨では、発行体や管理者が仮想通貨の価値を安定させ、維持することへの信用があることが条件となる。

## (2) 仮想通貨の分類

前記(1)の通貨の成立条件を現実の仮想通貨に当てはめるために、現在、仮想通貨と呼ばれているもの(現実に存在する仮想通貨と呼ばれているものは多様かつ毎日増加しているため、典型例を取り上げる)、銀行などの主体が今後発行を表明している仮想通貨、他国通貨(ドル紙幣)、国家通貨と過去の国家通貨(江戸時代の金・銀・銭貨)を以下の2点により比較して分類すると【図表2】のとおりとなる。

- |   |
|---|
| <p>A 保有・移転の排他性(コントロール)の有無(A-①技術、取引の正当性確認、A-②強制フォーク可能性(ファイナリティ)、追跡可能性(匿名性))</p> <p>B 発行体・管理者(帳簿管理など)の有無(B-①)、とその信用の有無(B-②見合い資産の有無、B-③発行量管理(希少性の維持や数量管理)<sup>17</sup>、交換所の有無<sup>18</sup>を含む)</p> |
|---|

a 発行体・管理者の観点からの通貨の条件  
以下、【図表2】をもとに検討を進める。ま

ず、上記Bの観点から通貨を整理すると【図表3】のとおりとなる。

ビットコインは、発行体および管理者はいない<sup>19</sup>がノード参加者のP2P内でのマイニングを、通貨として機能する信用の根拠としている。発行量上限は決められており、4年に一度新規発行額は半減し、このままのペースでは2141年に新規発行(マイニングの報酬)はなくなるとみられるほか、見合い資産はない。発行体、見合い資産がないので信用の源泉は、P2P内の信用(いい換えれば、マイニングの限界コストを通貨価値とし、その仕組みを維持していく「裏切らない」という顕示または暗黙の期待)しかない。この点、大多数の交換所の利用者はこの信用関係には参加していない。このため直接ノードを持たない利用者にとってビットコインは、P2P内の信用に依拠した仮想通貨とはいえない。ビットコインの価値が安定しないのは、こうした直接ノードを持たない参加者の急拡大と【図表3】に掲げたマイニングの難度調整が原因とみられる<sup>20</sup>。

NEM財団やイーサリアムのピアグループは、発行体または、帳簿や仕組みの管理者であるとは自ら表明していないが、イーサリアムがThe DAO事件でフォークを主導・実現したこと、NEM財団もコインチェック事件で犯人追跡のための工夫を講じ、フォークをしないと宣言したことは逆にフォーク能力を示したともいえる。利用者は、NEM財団やイーサリアムのピアグループを発行体ではないが、管理者とみる余地もある。法的責任の有無は別に、P2P参加者内で仮想通貨が「通貨として機能するための信用の根拠」になっていると思われる。

一方、いずれの仮想通貨も見合い資産がない

17 発行管理の希少性の維持とは、仮想通貨の発行残高や発行増額を制御する仕組みがあるか、またその制御が何によってなされるかが問題である。制御がないと流通実態に合わない大量の新規発行により価値下落の可能性が有る。

18 交換所の有無は、通貨の条件ではなく、P2Pに参加しないが、当該通貨を持っている利用者が存在することを示すために挙げている。

19 ビットコインのメンテナンスを進めているコア開発者以外にも、マイナーやウォレット開発者などがインターネット上で組織的に活動している。一方で、NEM財団は「財団」ではあるものの、その責務は教育や広報とされており意思決定機関でも保有者の利害調整の場でもないとしている。イーサリアムには、仕組みは似ているが、創始者個人の影響が大きい。

20 岩村充「ビットコインは難度調整をやめれば一人前の通貨に近づく」週刊金融財政事情2018年4月23日号36頁。



【図表 2】 仮想通貨の分類

通貨	(名称) ビットコイン*1	NEM*1	イーサリアム*1	各種アルトコイン、ICO通貨(イーサリアム等のプラットフォーム利用が多い)	銀行等発行*2 (?:MUFJコイン)	ドル紙幣	日本銀行券、硬貨	参考(江戸時代の)金、銀、銭貨 両(匁)、分、銭
	(単位) BTC	NEM	Ether			ドル	円	
法的 位置 付け	現在	仮想通貨		仮想通貨かつ金融商品	? (仮想通貨、前払式証券、預金のいずれか)	外国通貨 (金融商品*3)	(日本の)通貨	(江戸幕府公認の)通貨
	筆者の整理	P2P内信用仮想通貨(対ノード保持者のみ、発行体・管理者のない他の仮想通貨も同じ)	条件を整えば主体型仮想通貨	条件を整えば主体型仮想通貨	条件を整えば主体型仮想通貨または金融商品	主体型仮想通貨	国家通貨 (外国中央銀行)	国家(的)通貨 (中央銀行)
A 保有・ 移転の 排他性	①技術	UTXO(取引データ中未使用分計が残高)		UTXO+STATE(残高)	中央管理型のブロックチェーン	紙、印刷、流通	紙、印刷、流通	鉱山管理、刻印管理など
	取引の正当性確認の方法	確率的Proof of Work(POW)*4 : P2P間のPOWへの信用が根拠、逆にノードを持たない利用者の信用の源泉は過去使用されているという事実のみ	Proof of Importance*4 : 同左	Proof of Work、その後、Proof of Stake*4に移行予定。 : 同左	Proof of Stakeなどプラットフォームによる : 同左	エンドースメント方式 (NOTARYによる確認等): 銀行への信頼	紙幣の占有移転	紙幣、硬貨の占有移転 金貨、銀貨、銭貨の占有移転
	②強制フォーク	ありうる		あり(The DAO事件で実施)	ありうる?	—		
	追跡可能性	あり(事実上なしが判明) — 匿名性なし			可能 — 匿名性は当然にはない	なし(記番号管理せず、すれば可) — 匿名性あり	なし — 匿名性あり	
B 発行体 帳簿管 理者・ 管理者 と その 信用	①発行体	なし		なし、または、あり	銀行または信託	FRB	日本銀行、日本国	江戸幕府(金座、銀座ほか)
	帳簿管理者	なし	なし?	あり	?	—	—	—
	管理者	P2P集団(開発者、マイナー*5、交換所)あり	NEM財団は技術研究、広報が目的とする	P2P集団(開発者、マイナー、交換所)あり	(目論見書作成者またはその受託者である交換所など)	(FRBが発行管理)	(日本銀行が発行管理・硬貨は政府発行)	(江戸幕府が発行管理)
	②見合い資産	なし		なし、または、あり(資産または目論見書記載事業)	? (銀行または信託の資産)	FRBの資産	日本銀行の資産	なし
	③発行量管理	発行上限と4年ごとの新規発行額の半減期がある。	発行上限のみ(ただし上限は高く事実上青天井、半減期なし)	発行上限なし、半減期あり	(目論見書で発行計画の記載はあるが、追加発行を制約するかは確定的でない)	? (銀行の管理方針、能力による)		
	交換所	あり			?	銀行		各種両替商

\* 1 ビットコインは国家に依拠しない通貨を目指したものである一方、NEMやイーサリアムはブロックチェーンを活用したプラットフォームを目指したものとされており、開発目的やプラットフォーム上に搭載可能な情報が異なる。

\* 2 銀行が発行体または管理者となる仮想通貨の詳細は明らかでないため各欄は筆者の仮説である。

\* 3 外国通貨は、日常の貿易や旅行での決済に使わない日本人にとっては経済的には金融商品とみるべきとの学説が有力。

\* 4 Proof of Work: マイナーが、ブロックチェーンが正しく追加されたかを数値(ノンス)を総当たりで解読し、最初に解いたマイナーが12.5BTC(現在)の報酬(新規発行に相当するブロック接続権)を得るという解読行為をWorkとして、価値の保有・移転の正当性が証明されたと扱うこと。

Proof of Stake: マイナーが平等に競争すると暗号解読のための電力消費量が莫大になるので、当該通貨保有量と保有時間が長い保有者に既存履歴の正当性確認と新規のブロック接続権(トランザクション履歴に基づいて新たな記録の採用を決めるという考え方)を与える仕組み。電力節約になるが、当該保有者が不正しやすい点が指摘される。

Proof of Importance: Stakeと同様の発想で、当該通貨保有量と取引頻度の多い保有者に既存履歴の正当性確認と新規のブロック接続権を与える仕組み。

\* 5 マイニングプール参加者は含まない。

【図表 3】発行体・管理者の信用と通貨

B-①発行体・管理者	B-②見合い資産	B-③発行量管理	該当する国家通貨、仮想通貨
発行体なし、かつ管理者も責任主体でない	なし	あり（時間的な漸減）、ただし、短期的にはマイニング難度調整（10分で解けるように保つ）するため、供給量は増加しない、これが価格変動の一因とされる。	ビットコイン
発行体なし、かつ管理者からの表明はないが、管理者的に振る舞う団体、グループあり	なし	NEM：発行上限あり（ただし上限は高く事実上青天井、半減期なし） イーサリアム：発行上限なし、半減期あり	NEM、イーサリアム、アルトコインの一部
発行体あり（国や中央銀行への信用）	あり	あり（管理通貨制度）	中央銀行発行銀行券、外国通貨、ICOの一部、江戸時代の金、銀、銭貨、（銀行が発行または管理者の仮想通貨：詳細な発表はなく見合い資産があるか否か不明）

上、NEMの発行上限は非常に高く事実上青天井に近くかつ半減期の定めはない。またイーサリアムは発行上限がない。P2Pに参加していない利用者にとって、仮にNEM財団やイーサリアムのピアグループを管理者として信用したとしても、発行管理の仕組みが明確でないので通貨として価値が安定する仕組みが十分とはいえない。もともとビットコインと異なり国家への信用に依拠しない仮想通貨作りを目的としていないことから当然ともいえるが、発行管理（上限額などの発行額を使用実態などに応じて管理する仕組み）の現状では価値が安定するとは考えにくく、P2P内信用仮想通貨に該当しないというべきである。逆にNEM財団やイーサリアムのピアグループが発行体または管理者と自らを位置付け、発行管理を担うことで主体型仮想通貨と認めうる可能性がある。

こうした議論はアルトコインにも当てはまり、見合い資産がなく、発行管理もない場合には、通貨として機能することは考えにくく、見合い資産が何らかのプロジェクトであればIPOのような集団投資スキームと差はない。この点、現行法制は、詐欺的なICOは別として、アルトコインは、資金決済法と集団投資スキーム類似として金融商品取引法との両方の規律を受けると考えられるが、経済的実態にかんがみて整理することが適当と考える。

銀行や企業などが発行主体として発行する通貨または帳簿管理など価値の安定のための仕組みの管理者が存在する主体型仮想通貨では、利用者がその主体の存続可能性、流通実態に合わない大量発行をしないなどのルール遵守度を信用することが通貨として機能するための根拠になる。見合い資産の要否は、主体型仮想通貨の場合、必ずしも利用者と主体との間に個別事情による信用関係があるとは限らないとすると、利用するメンバーを限定しない場合には国家通貨に準じた見合い資産を持つほうがより信用されやすいと考える。

#### b 保有・移転の排他性の観点からの通貨の条件

次に上記Aの取引の正当性確認方法および強制フォークの存否の観点から通貨を整理すると【図表 4】のとおりとなる。国家通貨は、紙という性質にかんがみ、悪意の占有移転であっても所有権の移転になるという判例（前掲最二小判昭39.1.24）による実務慣行と、いったん発行された銀行券は無効にならないという信用がある。この点、ビットコインは保有や価値の移転の正当性の担保をP2Pの任意のマイナーが自由に競争して証明のための計算すること（マイニング）を皆で承認することに求めている。競争の勝者は悪意であっても少なくとも計算コストをかける必要があるほか、嘘の報告をして

【図表 4】保有・移転の排他性（正当性確認方法・強制フォーク）

A-①取引の正当性確認方法	A-②強制フォーク	該当する国家通貨、仮想通貨
マイニングによるPOW	ありうる	ビットコイン
マイニングによらない POI (NEM) POWからPOSへ移行（イーサリアム）	ありうる (管理者のようなものが存在)	NEM、イーサリアム、アルトコインの一部 ——イーサリアムはThe DAO事件後フォークを実施、NEM財団はコインチェック事件で追跡などを主導したほか、フォークは行わないと表明。
発行体、管理者（またはその指名者）による確認	ありうる	中央銀行発行銀行券、外国通貨、ICOの一部、江戸時代の金、銀、銭貨、（銀行が発行または管理者の仮想通貨）

もその検証が容易である。

一方、NEMのPOIやイーサリアムのPOSではマイニングは行われず、仮想通貨の保有者や取引回数や保有期間の長さを有する保有者が、新たな記録の追加を承認する方法で正当性を確認している。仮にそうした保有者が悪意である場合には、偽造や複製などが起き、その検証は容易でない。また、イーサリアムはP2Pやリーダーの主導のもと、The DAO事件後、強制フォークを実施したほか、NEM財団も強制フォークは実施しないと表明するなどして実施できる立場にあることを示している。強制フォークは、仮想通貨の過去の取引をなかつたことにすることであり、通貨としての信用を大きく損なう行為である。もちろん技術的にフォークは誰でもできるが、承認されなければ分岐は無効になるので、P2P内でのコンセンサスが必要になり、実際にはそうしたコンセンサスを得るだけの能力（事実上の強制力）が必要になる。逆にいえば、それをできることを示す団体や管理者のように振る舞うピアグループが存在する場合には、仮想通貨が通貨として機能するためにはそうしたピアグループが信用できるか（強制フォークしないか）が大きなポイントになる。他のアルトコインやICOもNEMやイーサリアムに準じて考えられる。正当性証明がマイニングによらず、既存の保有者の善意に依存する度合いが強いこと、強制フォークを主導して実現できる管理者またはピアグループがあること、からこれらの仮想通貨と呼ばれるものは、国家通貨同様に通貨として機能する条

件が十分でない面がある。

主体型仮想通貨も、ブロックチェーン技術を利用したとしてもマイナーは指定されるなど、自由競争によるマイニングで正当性を証明するわけではなく、結局こうした主体が、正当性を証明する仕組みを安定的に運営し、偽造や複製を監視していることに信用の根拠がある。強制フォークも技術的には可能であるが、それをしないことを約束するなど、あらかじめ利用者に表明するなどすることで通貨として信用されやすくなる。

なお、P2P内信用仮想通貨や主体型仮想通貨の利用者が自ら秘密鍵を管理せず、交換所や発行体・管理者に預けた場合（現実の推移は前記1のように、そうなることを予想させる）、現行のように寄託類似では支払手段としては機能しないが、消費寄託契約を結ぶと円の銀行預金類似の支払手段となる可能性がある。

以上をまとめると、仮想通貨が、通貨として機能するためには、価値保有や移転の正当性が担保される仕組みを有していること、強制フォークされないこと、価値維持のための発行管理がなされること（発行量・見合い資産管理）、これらを維持すると信用できる仲間（P2P内信用仮想通貨）または発行体・管理者（主体型仮想通貨）が存続すること、が条件になる。これを現実の仮想通貨と呼ばれているものに当てはめると【図表 5】のとおりとなる。

こうした理念形の仕分けが現実にはできるかは論点になる。仮想通貨と呼ばれるものの実態が通貨なのか金融商品にすぎないのかは、実際に

【図表5】 仮想通貨が通貨として機能する条件

仮想通貨と呼ばれているもの	「通貨として機能する条件」を満たす部分 ⇒国家通貨に関する規制と同等に規制すべきか要検討	「通貨として機能する条件」を満たさない部分⇒決済手段か金融商品か実態に応じて円建てと同様に規制すべきか要検討
ビットコイン	P2P参加者保有分	交換所利用者保有分
NEM、イーサリアム	なし（発行管理が明確でない、見合い資産なし、強制フォークありうる） ——ただし、NEM財団やイーサリアムのピアグループが発行管理ルールを定めるなど信用できる主体となれば全部が条件を満たす。	すべて
アルトコイン、ICO	ビットコイン同様の仕組みのあるコインのP2P参加者保有分（NEMやイーサリアムプラットフォームによるコインはそれに同じ）	左記以外のすべて 集団投資スキームとみなされるICO
銀行等の発行体、管理者のある通貨	銀行等が発行体として、または帳簿等の管理者として保有・移転の正当性確認、発行管理に責任を持ち、強制フォークをしないことを利用者に確約することが条件、見合い資産があればなお信用しやすい。 ——発行体が信託財産で見合い資産がある場合には、管理者（受託者等）が問題になる。	左記の条件を発行体や管理者が満たさない場合

※ 部分がP2P内信用仮想通貨、 部分が主体型仮想通貨

日常の取引の決済（金融商品としての売買ではなく、財やサービスの対価支払）に使われている程度で決まる。この点、P2P内信用仮想通貨や主体型仮想通貨を通貨制度の当局が認定するためには、決済金額と金融商品としての売買額を統計として把握し、決済金額の比率が高いこと<sup>21</sup>を最重要項目として、保有・移転の正当性確認の妥当性、発行管理（残高上限、増減額管理、過剰発行管理）、強制フォークの放棄等の条件を定めて定量・定性判断し、当局が利用者に情報公開することが適当と考える。国際的に通貨として機能するものであればG20など国際的な枠組みでの認定を行うのが適当である。もちろん、通貨は使う人が通貨だと信用すると通貨になるのでこうした指標でも使う人によって通貨になったりならなかったりする難しさを

承知の上で、明らかな場合には扱いを区別していくことが適当である（前記1(2)参照）。

（ながの さとし／瓜生・糸賀法律事務所）

21 中央大学・黒田巖元教授からご教示を受けた。江戸時代の一部の仲間内だけで通用した商人の手形や証文のように通貨として使われ、広がりがないければ、制度も必要とはいえない。P2Pが顔のみえる範囲であれば制度は必要がないともいえる。しかし、ビットコインのように発行時価総額が12.4兆円（2018年3月末）もあり、いろいろな決済に使えとなるともはやP2P内だけの規制だけでは足りないことになる。なお、古市峰子「現金、金銭に関する法的一考察」金融研究14巻4号101頁に、機能するものが現金という観点も踏まえた詳細な検討がなされている。