Summary

ブロックチェーン技術と通貨・証券の今後
～改正資金決済法・金融商品取引法を踏まえて～

弁護士法人 瓜生・糸賀法律事務所　弁護士・弁理士
長野 聡[1]

要約

■ 暗号資産と STO（セキュリティトークンオファリング）にかかる資金決済法と金融商品取引法が改正され、2020 年 5 月 1 日から施行された。盗難や詐欺などの病理対応のための規制強化であったこともあり、発行や取引が活性化する気配はない。

■ しかし、ブロックチェーン（BC）技術を用いた通貨や証券の発行流通には、プロの金融機関（預金取扱金融機関や証券会社）や中央決済機関（日銀、全銀システム、証券保管振替機構など）が担ってきた中央集権的な決済制度に対して、ネットワーク参加者である個人や非金融機関企業が分権的に自らのノードで権利の記録を分散共有しうる技術を持ったという意味がある。

■ 改めて整理すると、BC 技術には、以下の 5 つの特色がある。
特色 1「分権的記録」　：分権的にネットワーク参加者全員が保有
特色 2「中央集権機関不要」：中央集権機関が不要な分よりコスト安く
特色 3「最新情報」　：最新の
特色 4「多様な情報」　：多様な情報を
特色 5「履歴管理」　：履歴を連続させて記録し、
その存在を全員で検証できる。

■ この特色を踏まえると、今後 BC 技術を用いた通貨、証券の発行流通の形態には、日本の経済社会生活の転機にあって色々展開の余地がある。例えば地域通貨、ローカル（地理的なものに限らない、特定分野の仲間の間、宗教、趣味など）な資金調達のための STO が考えられる。こうした通貨や証券には、期間、金利、併合分割、移転制限、商流と併せた価値の移転など様々なカスタム仕様が可能となるほか、残高証明などで中央集権機関に頼らず、保有者自らが最新性と履歴を証明できるなどの点で画期性がある。

■ 物流企業や Fintech 企業の参入も必至であるが、既存の預金取扱金融機関や証券会社は、プラットフォーム提供などのビジネス拡大余地があるほか、資金繰り管理と融資を取扱う預金取扱金融機関には優位性がある。

■ こうした展望の前提は、スマホの基礎技術も含めたセキュリティの確保とプライバシー・個人情報保護のための技術的な対応である。こうしたことを踏まえて、イノベーションを促進するような法制度や法慣習の形成、さらには中央銀行デジタル通貨（CBDC）の在り方の検討も深まることを期待する。

[1] 前　日本銀行シニアリサーチフェロー

Ⅰ．問題意識

暗号資産（仮想通貨）と STO の法改正が 5 月から施行

暗号資産と STO（セキュリティトークンオファリング）に対して、消費者・投資家保護と公正な取引を確保する観点から資金決済法と金融商品取引法が 2019 年に改正され、今年 5 月 1 日から施行された。投機や詐欺的な資金調達を抑制するための規制強化方向の改正であったためか、国内では暗号資産取引は勢いづくことなく、また STO 発行もラッシュが続きそうにはない。一方でブロックチェーン（BC）技術をハンコなし契約、文書作成や証明書発行などに使う動きは活発になっている。

BC 技術の特徴と日本経済の構造問題とアフターコロナの相性

もともと BC 技術は、既存の特定の主体が運営する中央集権的なコンピューターのネットワークシステムに対して、ネットワーク内の情報の流れを「多から一へ」でなく「一から多へ」へ逆転させ、利用者全員が参加して、分権的に全員が記録保有し（特色 1「分権的記録」）、よって中央集権機関が不要な分よりコスト安く（特色 2「中央集権機関不要」）、最新（特色 3「最新情報」）かつ多様な情報を組み合わせて（特色 4「多様な情報」）、履歴を連続させて（特色 5「履歴管理」）検証可能な形で確実に移転するシステム技術である。それを通貨に使えば暗号資産に、証券に使えば STO、電子記録移転権利になるに過ぎず、脱地方・中央集権、東京集中、グローバリゼーションの明治以来の流れの中で完成された特定機関（日銀、全銀システム、証券保管振替機構、大手金融機関など）がコストは高いが効率的に通貨や証券の発行移転にかかる特定の情報を独占して集中管理する仕組みに対して、構造的な見直しを迫りうる、という視点こそが、目先の暗号資産や STO の展開を実現していくうえでも、今後重要と考える。

本稿の構成

本稿は、通貨と証券の今後について、資金決済法・金融商品取引法の改正の概要（第Ⅱ章）と BC 技術の特色（第Ⅲ章）を踏まえつつ、制度制約を別にして技術からみて今後どのように活用を展開させうるのか、自律分散社会での通貨と証券の展開、金融機関経営へのインプリケーション（第Ⅳ章）を論じ、BC 技術展開の留意点としてセキュリティ・BCP、プライバシー・個人情報保護、中央銀行デジタル通貨（CBDC）の意義について（第Ⅴ章）述べる。

技術変化と規制制度と企業組織の消長

結論を先取りすると、こうした技術変化と規制制度、そしてその変化を促す経済社会の変化というのは人類史の中で常に起こってきているという認識こそが大事なことと考える。金融（通貨と証券）の歴史だけをみても金属の時代、紙の時代、そして計算機と電話からそれらを結合したコンピューターネットワークの時代を経てきている。こうした変遷と問題の本質は、BC 技術であっても何も変わっていない[2]。大事な教訓は、経済社会とそれを支える技術が、プロの独占からアマがプロと同じことをできるように大衆化していくことで、既存秩序に甘んじて、経済社会生活が求めるニーズに応えないプロや制度は役割を終えていく、しかし全部が全部なくなるわけではない、ということであろう。

[2] 黒田巌（1987）「金融技術革新」東京大学出版会『日本の金融［Ⅰ］新しい見方』第 4 章

Ⅱ. 暗号資産と STO の制度改正（改正資金決済法、金融商品取引法）

1. 暗号資産（仮想通貨）と STO の制度改正

法改正による暗号資産と STO の峻別

昨年の資金決済法と金融商品取引法の改正[3]により仮想通貨は暗号資産（crypt assets の和訳）と改称され、BC 技術を使った証券による資金調達取引いわゆるセキュリティトークンオファリング（証券トークン発行、以下、STO[4]という。）は金融商品取引法の対象であることが明確にされ、暗号資産と STO は制度上峻別された。

暗号資産の法改正

その上で暗号資産については、利用者保護強化と他の金融商品と平仄をとるため暗号資産売買やその媒介取次を行う暗号資産交換業者に預かり暗号資産の分別管理や自己取引の規制などの規制強化が図られたほか、暗号資産のデリバティブズ取引[5]は金融商品取引法の適用対象とされ、資金決済法でなく金融商品取引法の規制対象となった。

STO の法改正による上乗せ規制

STO=
1 項有価証券のトークン化
＋電子記録移転権利（2 項トークン化で流動性高いもの）
＋適用除外電子記録移転権利（2 項トークン化で流動性高くないもの）

一方、資金調達取引では、BC 技術を使った有価証券、即ち株券や社債の発行、投資ファンドの資金調達（ファンド投資を BC 技術で有価証券としたもののうち流通性の高いものは「電子記録移転権利」と呼ばれ、金融商品取引法第 2 条第 1 項のいわゆる 1 項有価証券と位置付けられた[6]）が金融商品取引法の有価証券とされ、それぞれに開示、不公正取引の禁止、そして取扱業者規制に服する旨の制度改正がなされた[7]。STO に対する仲介業者規制は、従来の紙や保管振替による有価証券同様の部分が大半であるが、投資ファンドなどをトークン化する場合、流通性が高い場合には、1 項有価証券とされることで電子記録移転権利として、一種業者の募集、仲介が求められる一方、流通性が高くない場合（いわゆる適用除外電子記録移転権利）に開示規制や仲介業者規制の適用除外となる私募の要件は、BC 技術を用いるという特色に鑑みて、既存の 2 項有価証券同様に十分な資産を有している（個人は 1 億円以上の投資性金融資産等保有者に限る）ことに加えて移転の都度保有者申出と発行者の承諾を要するほか、BC 技術についての理解が求められること[8]、が上乗せされた。

---

[3] 2019 年 5 月 31 日に成立した「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律」（令和元年法律第 28 号）。施行は、2020 年 5 月 1 日。

[4] 起業時におけるブロックチェーンを使った資金調達取引であるイニシャルコインオファリング（資本性証券の発行、ICO と呼ばれる）も含める。これは未上場企業の株式公開をイニシャルパブリックオファリング（IPO）と呼ぶこととの類似性から名付けられたもの。

[5] なお、デリバティブズ取引は、原資産取引価格のボラティリティが価格の収斂の条件であり、それゆえに経済的意味があるのだから、原資産価格が投機でしか決まらない場合に、どこまで経済的意味があるか、筆者は疑問を持つ者である。

[6] 流通性の低いものは、金融商品取引法第 2 条第 2 項の有価証券とされた。流通性の高いものは電子記録移転権利として 1 項有価証券扱い、高くないものは 2 項有価証券扱い。この両者に加えて、金商法 2 条 2 項柱書にある 1 項有価証券のうち券面が不発行のもの（有価証券表示権利という）でブロックチェーン技術を用いて権利を移転できるものの 3 つを併せて、「電子記録移転有価証券表示権利等」と総称される。まとめると、STO＝法令上の電子記録移転有価証券表示権利等＝1 項有価証券（株券や社債等）をトークン化したもの（法令上の 1 項有価証券）＋流通性が高い 2 項有価証券をトークン化したもの（法令上は電子記録移転権利、1 項有価証券扱い）＋流通性が高くない 2 項有価証券をトークン化したもの（法令上は名前なし、適用除外電子記録移転権利と言われることがある、2 項有価証券の扱い）、となった。

[7] 金融商品取引法の改正については、金融庁の HP のほか、「セキュリティトークン・STO 規制の全体像」（増田雅史弁護士、金融法務事情 2020 年 5 月 10 日号（2137 号））がまとまっている。

[8] 自主規制団体である日本 STO 協会「電子記録移転権利等の取引等に関する規則」第 4 条第 2 項

図表 1：改正金融商品取引法で規定された BC 技術を使った資金調達規制の概要

<table>
<tr><td></td><td colspan="3">2 条 1 項有価証券</td><td colspan="2">2 条 2 項有価証券</td></tr>
<tr><td rowspan="2">有価証券の種類（金融商品取引法の発行等の定義による分類）</td><td>既存 1 項（株式、社債、地方債ほか、既存の電子化の場合（有価証券表示権利）を含む）</td><td colspan="2">STO（保振利用しない）＝電子記録移転有価証券表示権利等</td><td colspan="2">既存 2 項（集団投資スキーム持分等）</td></tr>
<tr><td>既存（有価証券表示権利）1 項（株式、社債、地方債ほかを BC で記録）</td><td>電子記録移転権利（投資ファンド等を BC で記録）</td><td>適用除外電子記録移転権利（通称）（投資ファンド等を BC で記録、一定の投資家［5 千万以上資本金法人、口座開設 1 年以上＋投資性金融資産・暗号資産合計 1 億円以上個人］で移転の都度、発行者の要承諾等）</td><td></td></tr>
<tr><td>発行者の開示規制が課される募集（公募と私募の境界［適格機関投資家私募、特定投資家私募、少人数私募は従来通り適用］）</td><td colspan="2">50 名以上の一般投資家に勧誘（49 名以下反復の場合を含む）
＋発行額 1 億円以上、ただし、国債、地方債は免除
電子記録移転権利は特定有価証券開示対象</td><td colspan="2">500 名以上の投資家が保有
＋発行額 1 億円以上
＋出資金の 50%以上有価証券投資（有価証券投資事業権利等）</td></tr>
<tr><td>私募の追加要件（転売制限）</td><td>一括転売以外の転売制限措置（契約）</td><td colspan="2">一括転売以外の移転ができないようにする技術的措置</td><td>なし</td></tr>
<tr><td>募集・仲介業者規制</td><td colspan="2">1 種業（クラウドファンディングは緩和）
株券・社債券の自己募集は業規制なし
電子記録移転権利の預託は要 1 種</td><td colspan="2">2 種業
集団投資スキームの業としての自己募集・私募は要 2 種（除く適格機関投資家等特例業務）
適用除外電子記録移転権利の預託は要 2 種</td></tr>
<tr><td>募集、売出し、売買時に勧誘できる投資家の範囲（勧誘するには有価証券届出書を財務局に要提出）</td><td>制限なし。ただし、非上場株式は適格機関投資家のみ（日証協規則、例外あり）</td><td colspan="2">上場銘柄は制限なし、非上場銘柄や PTS でない銘柄は発行開示すると制限なし。ただし、全銘柄で個人は BC 等を使用した商品について一定の知識等があるもの（監督指針ほか）。</td><td>一定の投資家（個人、投資性金融資産・暗号資産合計 1 億円以上保有者）、ただし、全銘柄で個人は BC 等を使用した商品について一定の知識等があるもの（監督指針ほか）。</td><td>制限なし</td></tr>
</table>

注：青字は要件上乗せ部分
出所：法令等から筆者作成

2. 制度改正の意義と限界

規制強化と盛り上がりを欠く発行、取引

法改正前には、暗号資産（改称前は仮想通貨）が投機から乱高下し、交換所から預かり通貨の盗難が相次ぎ、交換所の自己取引と顧客取引の併営による法外な利益など消費者保護に悖る事態になっていたうえ、ICO では詐欺が世界的に横行、日本の投資家が外国での ICO などに応募して喫損する事態となっていた。こうした事態に対処するために法改正は急がれたし、そのための規制強化と言える。この結果、暗号資産取引量は国内取引所では一時の勢いがないほか、STO 発行も私募範囲規制や保有制限から相次ぐとは見込まれていない[9]。

[9] 2020 年 6 月 22 日号週刊金融財政事情（新聞の盲点欄）「新たな資金調達『STO』、二次市場不在で商機見えず？」

そもそも BC 技術とは、また、その特色

一方で、BC 技術は、ネットワーク参加者が分散的に記録を同時に保有記録する（分散台帳）ことでシステムを運営する特定の主体（IT ベンダーなど、中央集権モデル）に頼らず、記録の真正性、唯一性、正当・存在性を確保できる[10]仕組みである（詳細は第Ⅲ章参照）。その特色は、

特色を踏まえて制度を超えた BC 技術の展開

特色 1「分権的記録」　：分権的にネットワーク参加者全員が保有し
特色 2「中央集権機関不要」：よって中央集権機関が不要な分よりコスト安く
特色 3「最新情報」　　：最新の
特色 4「多様な情報」　：多様な情報を
特色 5「履歴管理」　　：履歴を連続させて記録し

その存在を全員で検証できる、という点にある。IT ベンダーの寡占コストを節約し（当面ビジネス的にはこの面が強い、特色 2）、哲学としても自律分散社会にも適合できることから（将来的にはこの面が大きな意味を持つ可能性、特色 1）、帳簿その他の変化する記録、契約などに使われはじめている（特色 4、特色 5）。BC 技術の活用先を通貨や証券に限っても、海外では暗号資産取引は低調にはなっていないほか、Libra をはじめ見合い資産（裏付け資産）のあるステーブルコイン[11]の発行の計画が出てきている。また米国では STO の二次流通市場が、証券取引所と別に PTS（私設取引システム）で規模は小さいながらも運用が始まっている。

BC 技術の自律分散型組織にとっての意義

BC 技術による通貨や証券を、単に紙や既存のシステムから BC 技術による記録に置き換えただけと見る立場ではなく、BC 技術が、権利にかかる情報を預金取扱金融機関、証券会社や中央集権的な決済機関（以下、「従来機関」という。）を使わず、ノード参加者が自律的に発信し、皆で共有し、真正性、唯一性、正当・存在性を証明できる、さらに従来機関が提供している定型の取引形態だけではなく、他の取引と組み合わせてオーダーメイドの取引を展開できる道具を個人、中小企業、NPO、地方公共団体、自律分散型組織（DAO：Distributed Autonomous Organization）が手に入れたと見る立場もあり得る。こうした立場に立ち、通貨、証券のイノベーションを促進する観点からは、今回の制度改正は、一里塚と見るべきと考える。

3. 制度改正を受けて残る課題

イノベーションが起きつつあることに鑑みると、今回の制度改正によって積み残された課題としては以下のようなものがある。

制度改正とステーブルコイン、Libra や地域通貨

第一には、Libra や地域通貨といったステーブルコインの位置づけである。bitcoin や Ether（Ethereum のコイン）は発行代り金を運用する見合い資産がない点で金（gold）と似ている。一方で、価値の安定のためにはアンカーとなる見合い資産がある仮想通貨（暗号資産）が国外では発行されている。米国債が見合い資産とされ

[10] 記録の真正性は、第一に記録が正当な者により記録されていることは、電子署名などによることで、第二に改ざんされていないことは、記録を検証するための競争が行われ、不正は競争の過程で支持されず、最大量の計算をした者が記録を確定できることで、いずれも確保される（マイニングによりブロックの確定がなされる。マイニングのことを POW と呼ぶ）。次に、記録の唯一性、即ち矛盾する記録があった場合の一意的な記録の確定は、マイニングなどにより正しいブロックを特定する方法による。次に、正当・存在性は、過去記録との整合性を担保する仕組み（ハッシュチェーンの連続や UTXO の仕組み）により確保できる。

[11] 瓜生・糸賀法律事務所も地域通貨で見合い資産を銀行などが管理するブロックチェーンを使った仕組みについて特許を取っている（「暗号資産管理システム及び暗号資産管理方法」特許第 6651108 号）。新規性は、見合い資産の運用の仕組みがあること、運用の結果を通貨の金利にマイナスも含めて反映できること、運用額が発行額を下回った場合の償還制約が可能なこと、移転制限ができるシステム構成を備えていること、である。

ている tether が代表例で、今後発行可能性があるものとしては、Libra や地方債などを見合い資産とする地域通貨がある。Libra は G7 各国の国債などのバスケットを見合い資産とすると発表されているほか、小職の属する事務所が特許を持つ地域通貨は、発行体である地域 DAO が、地方債や地域企業の株式・債券をポートフォリオで持つことを想定している。こうしたステーブルコインが、資金決済法の暗号資産か通貨建資産[12]かは決着がついていない。仮に、償還時に国家通貨や通貨建資産で払戻す約定あるものは通貨建資産として暗号資産に入らないとすると、それは有価証券（STO）に該当するであろうか。通貨建資産が、有価証券か否かは当然には決まらず、勿論、金商法第 2 条第 1 項の有価証券ではないし、ステーブルコインが国家通貨ではないが支払手段や価値尺度を目指す通貨性を持つのであれば、第 2 項の投資ファンドのように収益を期待するものでもあるまい[13]。この点で、暗号資産と STO の 2 つを峻別しつつ、暗号資産は通貨建資産でないもの、と定義したことで通貨建資産、さらに通貨とは何かが逆に問題として浮かび上がったと考える。この点は BC 技術の特色のうち、「分権的に記録を検証可能な形でできる」（特色 1「分権的記録」による）ことで、権利の所在をモノがなくてもあるかのように明認できる（高札を立てる）ようにモノ的に扱えるようになった本質に関わっている。そうなるとその権利は、請求権であってもよいし、請求する相手がいない物権的な権利（民法上は財産権）の 2 パターンがあり、それらが流通するならいずれも通貨としての機能を持ちうるということである。（この点に関する米国の制度動向についてはコラム 1 ご参照。）

制度改正と対抗要件問題

第二には、STO の移転は、BC 技術によって行われるが、その移転にかかる対抗要件について、会社法やその他の法的な制度改正（保管振替の場合には、社債、株式等の振替に関する法律で移転の効力要件、善意取得などが法定されている）がなされなかった。このため STO の権利移転にかかる発行体への対抗要件、善意取得、抗弁の切断などは立法ではなく、トークン化された 1 項有価証券については会社法など既存法で、電子記録移転権利は慣習などに委ねられるかたちとなった。もちろん BC 技術には二重譲渡を発見し、いずれを勝たせるかを決めるルール（マイニングなど）があるが、技術上、事実上の問題ではなく、異例時や関係者が少なく結託したような場合における STO の移転について法的安定性を得るための慣習形成とその延長線上の立法などが今後の課題である。この点は、トークン化を BC 技術で実現する際に、トランザクションやブロックにどのような記録を残すかを工夫することで、事後に誰がどのようにその権利を把持していたかが、証明できればよいし、元来 BC はそういう技術だとも言える。目に見えない権利を形として記録して、権利の所在を一意的に決める方法として、国や中央集権機関（証券保管振替機構［株式、社債など］、日銀［国債］、銀行［預金］）が無謬を誇り、証明するという方法もあるが、そうでなく、参加者皆で証明しようという技術を法的にどう位置づけるかが問われているという認識が重要である。このことは BC 技術の特色のうち「分権的にコスト安く記録を検証可能な形でできる」（特色 1「分権的記録」、特色 2「中央集権機関不要」による）ようになった点と深く関わっている。

[12] 「通貨建資産」とは、本邦通貨若しくは外国通貨をもって表示され、又は本邦通貨若しくは外国通貨をもって債務の履行、払戻しその他これらに準ずるもの（以下この項において「債務の履行等」という。）が行われることとされている資産をいう。（資金決済法第 2 条第 6 項）

[13] 金融証券取引法第 2 条第 2 項第 5 号は「出資対象事業・・・から生ずる収益の配当又は当該出資対象事業に係る財産の分配を受けることができる権利」と投資ファンドの投資を表示する権利を規定し、収益または財産分配をメルクマールとしている。ここで財産分配はキャピタルゲインの分配を意味していると解される。

上乗せ規制とカスタムコントラクトへの発展

第三には、STO の発行と移転について、流通性の高い電子記録移転権利には、紙や保振によるものと同様に開示規制が残り、1 種業者（いわゆる証券会社）の募集、仲介義務が課せられる一方、開示規制の例外となる流通性の高くない適用除外電子記録移転権利の私募には、保有者に 1 億円以上の金融資産等の保有のほか移転時の発行者の承諾や BC 技術についての理解が求められた。これにより、業者を介さず、地域などで転々流通する、少額ロットの資金調達取引で、STO を利用することは、厳しい私募条件をクリアするか、DAO 等の発行体が 2 種業者となるほかなく、そう容易ではなくなった。詐欺的 STO、ICO は抑制される一方で、逆にさほど資産がなくても顔を見知った地域のために債券や投資ファンドに少額投資する、資金調達する（特色 1「分権的記録」、特色 2「中央集権機関不要」による）、証券発行にあたり資金移転、分割併合などをネットワーク参加者が従来にない型の取引により柔軟に行う（カスタムコントラクト、特色 4「多様な情報」による）、今誰が株主や債券保有者なのかリアルタイムで管理でき（特色 3「最新情報」による）、その履歴を把握する（特色 5「履歴管理」による）等を自らがノード参加者としてできるイノベーションを実現して行くには壁が残った。

＜コラム 1＞米国の制度動向が投げかける問題

米国では、暗号資産は、原資産の商品と位置づけられ、原油や穀物同様にその発行や取引自体には規制はないが、そのデリバティブズには CFTC（米国商品先物取引委員会）の規制がある。原資産の暗号資産の取引所規制は州の行政規制となっており、規制の厳しい州と緩い州がある。一方、STO は、ステーブルコインを含めすべて証券とみなされ、SEC（米国証券取引委員会）の監督の下におかれる。一方で、SEC は、証券概念に該当する投資契約（Investment Contracts）にあたるかどうか、を所謂 Howey テスト[14]によって判断している。資金の拠出者が、自らの努力ではなく、第三者の努力により（第三者の努力に対して、資金の拠出者は受身である）収益を得ることを投資契約のメルクマールとしている。さらに、SEC の最近のディスカッションペーパー[15]によれば、BC 技術や情報通信ネットワークを利用して資金を調達して、その資金を別に投資し、収益を得る場合だけでなく、支払手段や利用権（何かを購入したり、利用できる権利）を少しでも超えてネットワークの価値自体の増加に資するものについても、Howey テストの第三者による収益期待に含まれ得るとして投資契約にあたるとの解釈論を提示している。即ち、「他人の努力から得られる合理的な収益期待の有無を評価するに際して、連邦裁判所は取引の経済的な実際に注目している。裁判所は、金融商品が買い手により使われまたは消費されるために募集され、販売されるか否かを考慮している。」として、投資契約でないと判断する方向に傾く要素として、デジタル資産が、その購入者がネットワーク上で資産を使うよりも、これを超えてネットワークの

[14] 元の判例は以下の通り。
1. SEC v. Howey Co., 328 U.S. 293 (1946)
This definition was uniformly applied by state courts to a variety of situations where individuals were led to invest money in a common enterprise with the expectation that they would earn a profit solely through the efforts of the promoter or of someone other than themselves. ・・・・an Investment Contract, for purposes of the Securities Act, means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise. ・・・It embodies a flexible, rather than a static, principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.

[15] “Statement on “Framework for ‘Investment Contract’ Analysis of Digital Assets” (SEC Discussion paper, Bill Hinman, Valerie Szczepanik, April 3, 2019)
https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1

増価を期待しない場合を挙げている 。さらに暗号資産についても同じ考え方をあてはめ、支払手段となるものは投資契約でなく、投資契約と支払手段を区別しつつ、支払手段は、購入されるものの市場価値と相関関係が深いことを考慮要素としている。その上で、ネットワークやデジタル通貨の機能が、発展し続けているか、または改善し続けている場合に、そのネットワーク上での財やサービスの購入に使われることができる場合（支払手段と解釈できる）であっても、デジタル通貨が財やサービスの価値を割り引いて買い手に与えられたり、売られたりすること、デジタル通貨が合理的な使用を超える量で買い手に与えられたり、売られたりすることがあれば、それは証券取引になるとの考え方を示しているほか、特に第三者が、デジタル資産の価値増価のため努力を続けている、または流通市場を使い勝手を良くすることでネットワークの価値が増価している場合には証券取引とみる余地がある、としている。

即ち、発展途上のネットワーク上のデジタル通貨の増価期待があればそれは、支払手段であっても投資となりうることを示している。米国 SEC の悩みは、支払手段や価値尺度である通貨と証券、投資契約の区別が、技術の発展段階では難しいことである。米国の制度動向は、BC 技術を用いて、投資性と通貨性（収益よりも支払手段や価値尺度、ステーブルコインが典型）の双方を兼ね備える STO の発行があり得ると認識し、証券会社を介さず、企業、NPO、公共団体などが発行し、広範囲でなく流通する STO を積極的に登録させることで規制対象に取り込もうという方向にある。

4. 通貨、有価証券、ローカルな STO

通貨と有価証券の区別

特に通貨と有価証券の区別について敷衍すると、もとより、通貨は、国家通貨となる前は、最初は金銀など金属貨幣が、次いで信用ある主体の債務証書が、支払手段として決済に用いられてきたのが歴史である。この信用ある主体例が、英国の金匠で、金匠手形が支払手段として流通した。日本では伊勢神宮外宮の神職に就く伊勢山田商人が自治組織を作り、自らの資力と伊勢神宮の権威を信用のバックとして金銀の預り証文を発行、山田羽書と言われ、伊勢から中京地区で、日本最初の紙幣として流通した。こうしたものは見合い資産がある通貨と考えられる。また、中央銀行の紙幣や銀行の預金も見合い資産（兌換や償還義務はないが）となる国債や貸出がある。そう考えると、通貨と有価証券を法制で峻別することが妥当かどうかは、使う側の意識と用途次第ということになる。

二項対立ではない、通貨は機能による呼称

改正資金決済法では、暗号資産を「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」と定義し、ただし、通貨建資産は除くとしている。この定義は通貨の機能を定義したものであり、有価証券を通貨として利用することは想定されていない[16]。しかし、通貨と有価証券は、経済的機能としては二項対立するものではなく、通貨は、何かが支払手段や価値尺度として用いられ、かつ価値が安定していれば経済的には通貨として使われるという「機能」を表している。一方で、有価証券は、投資家が資金を拠出して第三者の働きによる収益（その程度は金利情勢や経済情勢によって様々、キャピタルゲインも含まれる［米国では判例、日本では金商法第 2 条第 2 項第 5 号］）を期待する（Howey テスト）金銭的価値の移転の仕組みを言い、そういう仕組みが守るべき開示、不公正取引規制や仲介業者規制が法

[16] 資金決済法第 2 条第 5 項「この法律において「暗号資産」とは、次に掲げるものをいう。ただし、金融商品取引法（昭和二十三年法律第二十五号）第二条第三項に規定する電子記録移転権利を表示するものを除く。」とされた。

制度である。投資を表象する有価証券が通貨、支払手段や価値尺度として機能するかどうかは、その有価証券の価値の安定や信用度によるので、通貨か有価証券か、と二律背反で比較すべきものではないということになろう。通貨は、価値の安定や信用度の観点から制度が決められるものであり、有価証券は、開示や不公正取引の抑止の観点から制度が決められれば足りるし、両者は必ずしも峻別されるべきものではない。さらに言えば、それが BC 技術によるものであるか、紙によるものであるか、金属によるものであるかも道具の問題であり、それが用いられる経済社会生活実態とそれに応えるための技術の内容により規制のあり方も当然に変わるべきものとなろう。その上で、通貨としては個人が安全便利に使えるものでなくてはならず、投資のリスクプロファイルが明確で、かつ転々流通が素人でも容易にできる技術ができれば、プロ業者の取扱いを求める理由はない。

第Ⅲ章以下の展開

以下では、今般の法改正が提起する通貨と証券の別々の制度枠組を揺さぶりうる深い問題を踏まえた上で、制度制約をひとまず置いて、BC 技術の特色（第Ⅲ章）、技術からみて今後どのように活用を展開させうるのか、自律分散社会での通貨と証券の展開、金融機関経営へのインプリケーション（第Ⅳ章）、留意点としてセキュリティ・BCP、プライバシー・個人情報保護、中央銀行デジタル通貨（CBDC）の意義について（第Ⅴ章）述べる。

Ⅲ．ブロックチェーン（BC）技術の 5 つの特色

5 つの特色

利用者全員が参加して、分権的に全員が記録を保有し（特色 1「分権的記録」）、よって中央集権機関が不要な分よりコスト安く（特色 2「中央集権機関不要」）、最新（特色 3「最新情報」）かつ多様な情報を組み合わせて（特色 4「多様な情報」）、履歴を連続させて（特色 5「履歴管理」）持ち、記録の存在を参加者が自ら検証できる点に従来のコンピューターネットワークの使い方にはない特色がある。

1. 複数コンピューターに同時にデータを送り現に共有できていることを確認する技術

特色 1「分権的記録」

BC 技術は、コンピューター同士を結ぶ通信ネットワーク（インターネット）をファシリティ（設備）として、コンピューターを占有する（クラウドでもよい）主体が、自らのコンピューター上の記憶部にデータを記録するのと同時に、同じデータを他のネットワーク参加者（ノードという）全員にも送信し（ブロードキャスト）、同じデータをノード参加者がその占有するコンピューターに記録するのが基本的な仕組みである。同じデータを参加者皆が同時、共時に持っていることを確認できることで、中央集権機関なしに皆でそのデータの正しさを証明できることに眼目がある。参加者皆が認知していることを正しいとみなす、誰か特定の権威者を信じるのではない点で、分権的であり、そのルールであるプロトコルを皆で決めれば自律的と言える。

特色 2「中央集権機関不要」

データの形式に約束事（プロトコル）があり、送信者を示す電子署名（暗号技術による）、データ内容とこれらを簡単な数字に置換えたもの（暗号学的ハッシュ関数[17]が使われる）で送信するまとまり（トランザクション）が作られ各ノードに送信

[17] ハッシュ関数とは、任意長のコンピューターのビット列から固定長のビット列（ハッシュ値）を生成する関数で、暗号学的とはハッシュ値から、そのようなハッシュ値となる元のメッセージを復元することが（事実上）不可能であること（原像計算困難性、弱衝突耐性）、同じハッシュ値となる、異

される、そして各受信者が、送られてきたトランザクションを複数入れる大きなまとまり（ブロック）を形成し、そのブロックが、過去のブロックと整合的で、唯一であることを証明する（プルーフオブワーク「POW」[18]と言われる）ことでブロックが確定される。記録の真正性、すなわち記録が正当な者により記録されたことは、電子署名などにより担保され、改ざんされていないことは、一か所だけ書き換えて POW と矛盾なく、かつ他の履歴の POW のコスト以上をかけて計算することは事実上不可能であることにより担保される。また、記録の唯一性、すなわち矛盾する記録があった場合の一意的な記録の確定は、POW、マイニングなどにより正しいブロックを特定する方法による。また記録の正当・存在性、すなわち、過去記録との整合性は、ブロックを形成するときに、前のブロックを表象するデータ（暗号学的ハッシュ関数で前のブロックの記録をハッシュ値とする）を次のブロックに取り込み、ブロックを連続＝チェーン化させることで確保できる。こうしたプロトコルによって、ノード参加者が自らデータを検証することがデータ、数字が信用される根拠になっている。

ノード参加者皆で検証し、データを持つということは従来のネットワークの中の特定の者（中央集権的な主体、中央銀行、銀行、保振など）がホストコンピュータを持ち、データの真実性、唯一性、正当・存在性の証明を一手に担い、プロトコルを決め、1 対その他多勢であったシステムとは、設計の考え方が異なり、かつ実務的にも大きな違いが出得る。特定の権威だけに頼らず、データを共有することで相互に証明するという共助的な設計は、資本主義的なビジネスよりもある分野での共通利益を持つ仲間内という自律分散社会となじみ易い。ルールも皆で決める直接全員参加がなじむ。現に Bitcoin や Ethereum は参加者のボランティアや特定のエンジニアを皆が信頼する形でプロトコルが決められている。

2. 常に最新情報を履歴も含めて参加者誰もが確認できる技術

特色 3「最新情報」
特色 5「履歴管理」

仮に株券を BC 技術で有価証券として発行すれば、ある時点で誰が株主かは、ネットワークのノード参加者が、自らリアルタイムで履歴も含めて分散台帳を有しているとすると確認でき、それを第三者に示せる。この最新性とブロックチェーン（記録が載っているトランザクションが入っているブロックが連続している、その連続が台帳になっている）による履歴の一覧性を参加者が自他共に示し得る点が BC の特徴である。株主の特定は、現在は株主名簿でなされているが、その特定は会社による名義書換の確定まで株主は自ら即時にはできない。仮に戸籍や住民基本台帳を BC 技術で作れば、3 ヶ月以内に取得した戸籍謄本や住民票を提出せよ、といったこともなくなるであろう、今現在の戸籍謄本や住民票をその場で履歴も含めて住民が参加者なら市役所に行かなくとも、提出先に対して自分で提示することができる（もちろん反応速度、ノード参加者に誰もがなるような仕組みなど解決すべき点は多いが）。

なる 2 つの元のメッセージのペアを求めることが（事実上）不可能であること（強衝突耐性）等の性質を持つものを言う。

[18] POW の方法は種々あるが、Bitcoin では、正当なチェーンを確定するためのマイニングを行い報酬を得る誘因から、目標となるハッシュ値を見つけるために総当りの計算をする作業（マイニング）を行い一番早くその数値（その数値に実社会と関係する意味はない）を見つけた（それだけ計算のための電力を使った）者が、そのブロックを締め切り、確定させることができる。その作業を POW と呼んでいる。このことで一番コストをかけたもののブロックが正しいというプロトコルが実現できて、ブロックチェーンの唯一性が担保される仕組みになっている。この計算はノード参加者が中央集権的に誰かから命じられて行うものでも、協力して行うものでもなく、自発的に報酬欲しさから計算し、それが結果として、競争となり、分権的に唯一性の証明がなされる、この創発（emergent）コンセンサスがナカモトサトシ氏の画期性と言われている。

3. データの内容を合意で決められる技術

特色 4「多様な記録」

さらに重要なことは、データにどのような内容を持つかどうかも参加者の合意で決め得ることである。データの内容とその組み合わせ、トランザクションの構成、ブロックの構成に制約はない。また、プロトコルを前提に、トランザクション同士を組み合わせることもできる。各ノード参加者が自分でそうした新しいデータの送信によるいわゆる「カスタムコントラクト」を工夫し、それを参加者の同意を得て実施する、その可塑性、発展性が自律分散社会では大きな意味を持つ。勿論、そうしたノード参加者をサポートするための技術的な支援は不可欠である。例えば、カスタムコントラクトの型を作るためのエンジン（ひとまとまりの特定の機能やサービスを提供するソフトウェアやシステム）の存否とその柔軟性の程度が、その BC 技術がノード参加者の属する社会において発展できるかどうかの鍵となろう。

金融商品設計の自由

例えば地方債を考えても、現在の保管振替によるものでは、法的行政的な制約の下で多様な商品性がある訳ではない。しかし元来、債券も、金利、期間、いろいろな償還その他のオプション、移転制限、保有者毎の固有のサービス（移転制限など）も投資家ニーズに合わせて発行者が債券の設計をすることができてよい。顧客ニーズに合わせた商品設計をすることには、制度制約以外に技術面からコスト、システム開発などで時間がかかるという面はあるが、制度に自由度を設ける[19]ことが、BC 技術を活かす必要条件になるのではないか。第Ⅱ章で述べた現実の暗号資産取引や STO 発行規制はこうした視点で今後、規制緩和の余地があると見る。各ノードをサポートする立場にあるプロのビジネス側（既存の預金取扱金融機関や証券会社）はその特徴を活かすための技術を用いたサービス供給を考えることが求められている。

4. BC 技術の比較

Bitcoin、Ethereum の二大オープンソースが基準に

ノード参加者が、自主的にトランザクションやブロックの内容を提案し、コンセンサスを得て、カスタムコントラクトを作るためのエンジン（これがないとノード参加者は一から自分で仕組を作る、または出来合いの取引しかできず、ニーズに対する柔軟性が制約される）の有無と柔軟性の程度は、種々の BC 技術の中で、自律分散社会に資するという点で重要なポイントである。BC 技術には、枯れた Bitcoin、規模の経済を得るために POW の方法が大きく見直され、Proof of Stake（POS[20]）へ移行する予定の Ethereum は、オープンソースであり、かつ独自のエンジンを持っていることから両者が、BC 技術のベースとなるであろう。

コンソーシアム型との使い分け、共存を模索する戦国時代

こうしたオープンな BC 技術のほか、大手ベンダーや BC 技術企業が提供する私的な BC 技術（private chain）も Hyperledger Fabric（IBM 社）などが提供されており、独自のエンジンを持つものもあればそうでないものもある。私的なチェーンを持つベンダーや金融機関などが中央集権機関に準じてプロトコルを提供し、真正性、唯一性、実存・正当性を証明するのであれば、上記で述べたような特色は大きく減殺されてしまう。オープンソースの BC 技術やその改良型にせよ、コンソーシアム

[19] 「日米の STO 形成過程への感想」（第一生命経済研究所顧問、大森泰人、週刊金融財政事情 2020 年 6 月 29 日号）で大森氏は、「ルールのプリンシプル化」を主張しておられる。筆者も BC 技術と経済社会生活の展開をみて同意見を持つものである。

[20] Proof of Stake とは、大きな残高を持つノード参加者が残高比例で正しいチェーンを決める権利を持つ方法。計算負荷をかけた者によるマイニングによってチェーンの唯一性を確保する POW とは発想が異なる。

型にせよ、エンジンにより、ノード参加者が自らが求めるサービスを提供できる自由度、裁量があることが、BC 技術が発展し、経済社会生活に資し得るか否かの判断の分かれ目になろう。この点、まだ BC 技術の戦国時代は続いており、発展途上の技術という側面がある。

図表２：BC 技術のプロダクトとの比較

	構造の特色			将来展開の余地			指摘されている問題点		
プロダクト（ベースとなる技術）、開発者、特色、言語、エンジン	タイプ（フロー UTXO か口座残高 Account か）	ファイナリティ（トランザクションの確定）	台帳アクセス	スループット（反応速度、可用性）	インターオペラビリティ ⇒他のチェーンのコイン・証券との交換 DVP 可能	ネイティブトークン（固有通貨の有無） ⇒資金決済 DVP に対応容易	権限設定の容易性 ⇒組織内権限分配に対応容易	Pruning（不要な過去取引の刈込可能） ⇒適正規模維持による可用性維持	
Bitcoin（Bt） オープンソース、単純、枯れた技術 Bitcoin Script 独自エンジン	フロー	Proof of Work（計算コストでコンセンサス）	○ 参加者全員	× （セカンドレイヤーと結び処理は可能）	○ （アトミックスワップ等枯れた技術あり）	あり	×	○	・規模の利益なし ・改革の意思決定できない
Ethereum（Et） オープンソース、創始者の影響強い Solidity 独自エンジン	残高	同上（今後、保有者多数決 Proof of Stake 等に移行予定）	○ 参加者全員	× （セカンドレイヤーは後付け）	○ （同上）	あり	×	×	・Ether コイン使用が前提 ・ブテリン氏の独裁 ・コンセンサス方式変更（POW 放棄）の成否不明
Tapyrus （Bt ベース） chaintope 社開発 Tapyrus Script 独自エンジン	フロー（スマホ等軽量のクライアント可能）	運営者検証	○ 参加者全員	△ Bitcoin に同じ、設定で改善可	○ （同上）	あり （bitcoin ベース）	×	○	・Bitcoin の問題改善、ただし、コンセンサスは POW によらない ・ユーザー参加のオープンプラットフォーム向き
Quorum （Et ベース） JP モルガン社など開発 Solidity Ethereum エンジン	残高	運営者検証	× （指定参加者）	△ （仕様による）	△ （交換ツール開発中）	あり （Ether ベース）	○	×	・Ethereum の影響を受ける
Highperledgerfabric,IBM IBM 社独自開発 Go/node.js/Java Chaincode エンジン	残高	運営者検証	× （指定参加者）	△ （仕様による）	△ （交換ツール開発中）	なし	○	×	・デプロイ可能なロジックの数に制限あり ・長期的なスケーリングは、チェーンコードとチャネルの設計の影響を受ける
Corda, R3 独自社開発 Java/Kotlin Java エンジン	フロー	運営者検証	× （指定参加者）	△ （仕様による）	△ （交換ツール開発中）	なし	○	×	・転々流通時の検証コスト増大の可能性大

出所：各種情報から筆者作成

Ⅳ. BC 技術の活かし方

需要は創り出すもの

情報産業である金融機関への影響はより大きく出る

BC 技術も道具であり、通貨、証券の発行や流通にかかる既存技術を供給サイドで一部置き換える意味があるとしても、上記 5 つの特色を求めるような経済社会生活上の需要、ニーズが問題になる。故本田宗一郎氏は、大衆は何が欲しいかは言ってくれないが、良い製品が出るとこれが欲しかったと言う、との趣旨を本に書いておられる。今の当たり前はそうでない、需要はそこにあるのではなく創り出していくということを示していけるかどうか、通貨、証券のプロである金融機関が逆に問われている。技術の特色はプロが中央集権的に行っていた情報管理を個人や非金融機関が仲間内でできる点にあることから、金融機関のライバルは、物流や Fintech 企業でもある。経済社会生活の変化は、BC 技術の 5 つの特色を活かすことをどのように求めているか。事は記録全般に関するので活用は金融分野に限定されないが、もともと預金通貨、証券といった請求権という形のないものを扱っている、いわば情報技術を梃子として成長してきた金融業では経済全体の平均よりも情報技術の変化は早く、かつ大きな影響が及ぶ筋合いにある。筆者に通貨、証券分野への活用可能性を網羅的に列挙する能力はないので、特色を踏まえた現段階であり得べき例を示す。

1. 分権的記録を権利移転の効力・対抗要件とする暗号資産、STO、ステーブルコイン
―特色 1「分権的記録」、特色 2「中央集権機関不要」に基づく

流通範囲の狭い地域通貨、ローカル企業の資金調達手段としての STO

中央集権的な機関である銀行やそのネットワークである全銀システムや集中決済制度や大口資金移動を行う日銀ネット、さらに株式、社債など有価証券の移転を記録する証券保管振替機構の特色は、無停止、ほぼ無事故、さらにエラーがないうえに、即時に記録し、24 時間近く 365 日稼働できる世界に冠たる決済システムである。その恩恵を日本人や日本企業はフルに受けている一方で、完璧な分、莫大な開発維持運営コストがかかっており（コラム 2 参照）、新幹線などに似ている面がある。さらに言えば、決まったことしか対応できず、ネットワーク参加者が創意工夫で開発する余地はない。新しい機能の付加には何年もの調整準備、開発期間がかかる。参加金融機関の分担金負担も大きい。しかし、その中央集権的決済システムを使わないでも BC 技術を使って分権的な記録により権利移転を証明できる、法的にも慣習法により分散台帳記録が対抗要件になるという有価証券、特に地域通貨（暗号資産またはステーブルコイン）、流通範囲の狭い仲間内での資金調達としての STO の発行ニーズが、ローカルな（必ずしも地理的地域とは限らない、特定の分野、宗教、半分事業半分趣味などもあり得る）NPO や DAO、中小企業にはある。預金取扱金融機関にはステーブルコインなどと円資金との交換、さらに見合い資産管理、資金繰り管理、融資、また証券会社には STO などのプラットフォーム提供をビジネスにすることが考え得る。

＜コラム 2＞日本における通貨、証券決済の中央集権化

資金（通貨）の決済は、江戸時代は分権的であったが、明治以降、銀行が設けられ、そのコルレス関係を通じて資金の都市集中、その裏には工業化と人口の都市集中が進んだ。その後、昭和 18 年の内国為替制度によって、二銀行間のコルレスによる為替から日銀当座預金での一時点の集中決済制度が始まり、金利が全国で統一されていく（それまでは東京、大阪、名古屋、門司など各々に短期金融市場があった）。昭和 48 年に

は全国銀行データ通信システムが完成し、昭和 63 年の日銀ネット稼働により、短期資金取引の資金移動効率は一段と高まった。米国の Fedwire が一部の小口決済、小切手決済まで担っているのに対して、日本では日銀ネットが大口、全銀システム・各地手形交換所が小口と棲み分けている点が特色である。

国債や株式の決済も昭和 55 年の日銀の国債振替決済制度、平成元年の日銀ネット化、そして株式については昭和 47 年の証券取引所の子会社が運営した株券保管振替制度、その後、昭和 59 年の株券等の保管及び振替に関する法律が制定され、平成 18 年には一般債振替制度、平成 21 年には株式振替制度のシステムが稼働を始めた。

これらは、通貨や証券を決済する機関に記録を集中し、その記録を資金や有価証券移転の効力要件とする制度的な意味を持ち、未決済残高を圧縮してリスクを小さくしつつ、資金や有価証券の決済スピードを速め、効率利用することに狙いがあった。その後、コンピューターの処理速度の制約が小さくなるにつれ、集中決済制度で取られたネッテイング（貸借相殺）が当事者倒産時に巻戻しリスクがあることから、即時グロス決済（RTGS）、有価証券と資金の同時決済（DVP）が標準とされた。このため日銀ネット、全銀システム、証券保管振替機構、さらに個別銀行や証券会社のシステム投資は大きなものとなっている。

2. 通貨や証券の現在高、履歴証明の即時化、最新性保証[21]
ー特色 3「最新情報」、特色 5「履歴管理」に基づく

即時に、金融機関に依頼せず、保有者自らが現在残高を取引相手等に表示可能

ネットワークのノード参加者は、前第 1 項のようなステーブルコイン、STO のみならず、既存の預金や株式、社債等の有価証券を BC 技術で管理することにより、自他の現在保有高や移転履歴を自ら、中央集権機関の協力によらずに、即時に知り、証明することができる。中央集権機関である銀行や証券保管振替機構、証券会社に証明をしてもらうと何月何日現在高の証明はできるが、残高証明提出先に今現在の残高を即時に提示できるわけではない。弁護士経験に鑑みても離婚、相続や破産などの局面で残高が不明で金融機関の協力を得るには色々な手続きを踏まねばならず、かつ金融機関や証券保管振替機構が証明してくれるのは、ある過去の時点での証明であり、刻刻の履歴を即時まで証明してくれるわけではない。保管振替の階層構造では余計に時間がかかる。これを保有者自らまたは他の参加者ができると大きな社会的コストの削減になる。有価証券の保有者がある時点での保有証明を過去に遡った履歴も含めてできることは保有期間の利子課税などを経過利子などを使わず簡便にできると考えられる。

3. 有価証券の権利内容（商品設計）の柔軟と変更の迅速化
ー特色 3「最新情報」、特色 5「履歴管理」に基づく

商品設計の多様化と他の目的の利用

現在の有価証券の発行、移転においては、満期設定、単位、さらに銘柄併合や分割の手続には時間がかかる。しかし Bitcoin ベースの UTXO などによれば、最小単位（例えば額面 1 円）を決めれば、どのようにも分割、併合の取引も可能であるほか、満期も 1 日単位、1 時間単位、また利子も連続複利、半日複利、特定者への移転制限など様々なオプションを付し得る。このことは、資金調達取引の柔軟性を低コストで増すことができることを意味する。さらに株主名簿や社債原簿を分散台帳で作れば、株主総会や社債権者集会の議決権者の確定、定足数充足の計算、議

[21] 早稲田大学・岩村充教授から示唆を受けたもの。

決そのものを BC 技術を用いて行える可能性もある。

4. 通貨、証券と商流情報を組み合せた発行や移転 ―特色 4「多様な情報」に基づく

商流情報と組み合せた発行や移転

既存の通貨、証券システムでは、円と国債の DVP（同時決済、日銀ネット）、円と社債の DVP（保振ネット等）など特別に作成したシステムでなければ異なる通貨や証券を組み合わせて同時に移転することはできない。また、通貨や証券の移転とその原因取引に関する情報を併せ送信することは、型にはまったものや一定範囲のメッセージ送信しかできない。そうした仕組みとしては、例えば日銀ネットの付記電文、全銀為替の給振、年金振込などのタイプがあるほか、2018 年には全銀為替の情報に商流情報を付加できる全銀 EDI システムが稼働し[22]、資金振込の際に添付できる情報量は増えた。しかし、資金の振込に情報を付加するものであるため、商流にかかる見積⇒発注⇒納品⇒検収⇒代金請求⇒支払⇒領収書といった一連の流れを同じシステム内で資金決済の前や後の段階で相手方とやり取りすることや特定取引先との過去の取引を併せて情報をやり取りする仕組みではない。こうした取引先間の情報の往来は金融機関よりも物流、商流情報を持つ小売業、ネットでの販売業でニーズが強く、自社開発または Fintech 企業と組んで、持っている商流情報に加えて、決済情報を取り込む先も多い。金融業、商業、間を取り持つ Fintech 企業の間で取引前後の関連する商流情報のやり取りや別の取引と併せて資金決済をするサービス提供の競争が広がりつつある。BC 技術を使うことで、通貨や証券の価値移転のトランザクションに併せて、BC 上での契約を結び、その他の関連する発注等の情報を併せて送ることを、中央集権機関に頼らずネットワーク参加者が自らの相手方との取引関係に応じて作成できる、またその BC 技術が第Ⅲ章で述べたように固有のエンジンを持っていれば、そのようなトランザクションを各ネットワーク参加者が自分でカスタマイズして作りだすことができると考えられる。

金融機関のアドバンティッジとしての資金繰り管理と融資

こうした通貨、証券の決済取引と商流情報を結び付けることができたとしても、預金取扱金融機関は、物流企業や Fintech 企業にはない有利さを有している。即ち当座預金管理により個人情報保護に悖ることなく資金繰りを管理できるほか、融資ができることで収益チャンスがある。商流情報は、リテール、Fintech 企業の場合には個人情報保護、マネーロンダリングの扱いが問題となるほか、融資はできないので、銀行の M&A が今後こうした視点で行われることは考えられる。もとより、通貨や証券の移転は、理由があり、従来資金使途は返済可能性確認のために問われてきた。通貨、証券の歴史をみるとカネに色はついていた、決済と貸借、いずれも期限が到来するまでの関係性が背景にあり、どういう場合に、誰が、どこで、何ができるのか、についてはその属する社会のルールがあった。そのため信用コスト管理、資金繰り管理のプロである預金取扱金融機関の存在意義がある。このためローカルな通貨や証券が BC 技術でできても地域金融機関の存在意義がなくなるわけではない、商流情報を自らプラットフォームを作り握ることは、与信管理には大きな意味を持つ。貸借関係は、その時だけの関係ではなく、過去から未来までの交渉がある関係であり、そうした履歴があることが BC 技術の履歴管理とも相性がよい。

[22] ZEDI は 2018 年 12 月 25 日に稼動した。企業間の振込電文について、固定長形式から国際標準である XML 形式へ移行し、総合振込の際にそれまでの固定長形式で 20 桁までから、多くの情報を自由に設定することができるようになった。支払通知番号や請求書番号など、商取引に関する情報（商流情報）を添付可能となり、大きな進歩となった。

Ⅴ．セキュリティ・BCP、プライバシー・個人情報保護、中央銀行デジタル通貨（CBDC）、他の論点

BC 技術を活かした通貨、証券の価値保有、移転を発展させるには、以下のように解決すべき重要な論点がある。

1. セキュリティ・BCP

BC 技術の採否は、セキュリティ、BCP、技術進歩予測も踏まえて要総括判断

BC 技術を使って通貨、証券を発行移転することが真にコストがより安いか否かは、セキュリティや可用性、BCP 対応（障害時対応）まで含めて総括的に技術進歩も見通して判断する必要がある。可用性についてはプライベートチェーンでは改善がされる一方、パブリックチェーンでネットワーク（ノード）参加者が増えると反応は鈍くなる。この点、金融市場での大口の裁定等取引には現時点では向いていない。セキュリティについて、ハッシュ値などが解読される可能性は、過去の取引については量子コンピューターの開発等により、コンピューターの計算速度（解読性能）が上がればあり得るが、高速化するにつれて暗号の作り方も高度になるので、今後の取引について解読される可能性は低い。しかし、プライベートチェーンではシステム運営主体による改ざんなどのリスクが残れば、中央集権機関による管理運営コストやセキュリティ管理との相違は程度問題になる。BCP については分散台帳ではノード参加者の一部が被災、事故にあっても他の台帳から復元できるとするとレジリアンスは高いとみられる。ただし、インターネットの障害、プロバイダーを含めた通信キャリアの障害の影響は大きく出ることから、事前の BCP 対策が必要になる。

2. プライバシー・匿名性、個人情報保護とマネーロンダリング

情報共有とプライバシーの背反性

自律分散社会の前提は仲間の間の信頼である。その仲間の間、ノード参加者間では情報の共有が、その情報＝データの真正性、唯一性、実存・正当性の証明の基礎となる。それは個人情報保護と匿名性要求、さらにマネーロンダリングと背反するであろうか。信頼できる仲間にも情報を見せないということは、自律分散社会の考え方には合わないところがあり、信頼すれば情報を共有してもよいとも考えられる。もちろん分散台帳における情報に誰がどこまでアクセスできるかを事前制限し、記録を残す BC 技術は進化しつつある。しかし、仲間内でだれが何を知っているのかを共有するということについては、どのような経済社会生活の道具として BC 技術を利用するかという問題と深くかかわり、そのネットワーク参加者内で慎重に決めるべき問題であろう。

ケースに応じたアクセス制御の技術が必要

特に通貨や証券ではこの問題は重要な意味を持っている。通貨と証券の歴史は、その流通範囲を広げつつ、仲間うちから、経済社会の参加者であれば、知らない相手にも転々流通して、実取引と関係なく決済が円滑に進む方向に進んできたが、ここへきて、取引におけるプライバシー保護、個人情報保護、マネーロンダリングの抑止が国際的な社会課題となっている。むしろ通貨、証券の使われる範囲を、対になる実取引と結び付けて制約をかけよう、そのためにプロである銀行や証券会社に本人確認、個人情報保護にかかる金融機関向けの特則などでより厳格な責任を課そうというのが世界の規制の潮流にある。通貨（預金を含む）、証券の移転時において取引当事者が、第Ⅳ章 4 項で述べたように商流情報とその履歴を持つことに意味はあるが、分散台帳で共有することは常に適当とは思われない。また証

券発行を入札などで行う場合には、入札参加者や入札価格も秘密にしないと入札が機能しない。BC 技術と自律分散社会において通貨、証券の在り方を考えるうえで、ネットワーク参加者間で合意されるプライバシーに応える BC 技術や関連アプリケーションの提供が、今後、プロである預金取扱金融機関や証券のビジネスを考えるうえで重要とみる。

3. 中央銀行デジタル通貨（CBDC）

銀行券が残るならユニバーサリテイは完璧である必要はない

BC 技術を用いた暗号資産やステーブルコインが発行流通し、商流情報を組み合わせたサービスが提供されたとしても、デジタルデバイド（積極的にアクセスしない人を含む）やセキュリティ懸念ゆえに現金（銀行券）が完全になくなることはない。一方で国民、国家的信用を背景にした公的なデジタル通貨へのニーズもある。預金取扱金融機関や仲間内の BC 技術による通貨も取引先や仲間内を越えて日本、世界と取引するニーズはあるが、私企業は倒産しうるし、信用できる仲間でない相手との決済には、信用度の高い通貨は不可欠である。このため世界の中央銀行が中央銀行デジタル通貨（CBDC）を検討する理由はある。この点、日銀が 2020 年 7 月に発表したペーパーでは、CBDC が現金同様の機能を持つためには「ユニバーサル・アクセス（Universal access）」と「強靭性（Resilience）」を備えることが望ましいとされている[23]。前者は現金（日本銀行券）が残るのであれば完璧である必要はないので、世界的な通貨競争の中で開発供用スピードとの兼ね合いが必要であろう。後者は華為技術を巡る各国動向に鑑みても、スマホの基礎技術のセキュリティ確立が大きな課題であろう。

CBDC 移転に伴う情報付加は利用者の選択肢であるべき

日銀による情報取得は通貨機能を一部損なう

一方、日銀ペーパーが指摘するプライバシーの確保と AML/CFT への対応は難しい問題である。日銀券保有の安心の源泉は、中央銀行組織と国民、国家への信用であるほか、銀行券の匿名性や取引情報から独立しているという点も大きい。阪神淡路や東日本大震災などで現金保有の安心が指摘されている。元来通貨決済は取引関係、信用関係の履歴と切り離せないし、その点で BC 技術などがメリットを発揮できる点があるが、履歴と切り離されて即時に使えるという流動性があることは経済社会生活上の意味がある。通貨がプライバシーと切り離される点は AML/CFT とは相容れない面がある。こうした銀行券の性格を維持するのであれば CBDC で、中央銀行が利用者間の情報を積極的に取る必要はないし（一方で利用者が CBDC の移転に情報付加を望む場合にこれを排除する必要もない）、AML/CFT に関与することは通貨の機能を一部損なう面があることに留意すべきであろう。

4. 他の論点

他の論点をすべて検討する紙幅がないので列挙するに留める。

法制度のあり方と商慣行形成には時間、抵触法の側面は急ぎ検討を要する

第一には法制度の在り方がある。まず行政規制・自主規制としては、手段が紙でも保管振替でも BC 技術でも有価証券の扱いという点では原則として平仄を取ることが適当と考える。次に BC 技術の下で通貨と証券の区別は明確に峻別できるとは言えない。通貨は機能であって規制のための証券という概念とは必ずしも同じ土俵で二項対立する概念ではない（第Ⅱ章参照）。その上で通貨規制、証券規制さらには商品取引規制の体系を見直す余地がある。技術進歩に伴うイノベーションを促進するためにはプリンシプルベースの行政がこの分野には相応しいと考える。

[23] 2020 年 7 月　日本銀行決済機構局「中銀デジタル通貨が現金同等の機能を持つための技術的課題」

さらに自律分散社会における BC 技術による通貨、証券の価値保有や移転について差押、破産といった対抗問題と相続、合併などにおける財産の存在の確定などの慣習法形成の在り方が実務と判例を通じて形成されることが期待されるが、日本社会の法形成の在り方にも通じる難問と思う。そのうえで BC 技術による通貨や証券の価値移転は国境を越える。銀行間のコルレスバンキングについて国際連合国際商取引法委員会（UNCITRAL）が提示したネットワーク責任論が BC 技術による場合にはどうなるのか等、対外取引については深めるべき論点は多い。

預金取扱金融機関の意義

第二に預金取扱金融機関と証券会社の区別は、預金と融資という 2 点を除いては、境界はさほど明快ではなくなると予想する。ユニバーサルバンキングを志向するというよりも、Fintech 企業や物流企業の参入による周辺業務や商流情報は、いろいろな業種が取り込みを図るであろう。預金取扱金融機関は、資金繰り管理と融資の 2 点を深めることが他業態にできないポイントであろうが、システムを含めてこれらの点も外堀が埋まりつつあり、座しているだけでは失地は必至である。なお、こうしたことがマネーの定義、金融政策の中間目標や手段に影響があることは言うまでもなく、状況に応じた判断が必要になる。

Ⅵ. おわりに

日本の経済社会生活の構造問題とアフターコロナ

明治以来日本は中央集権化を強める国づくりを行ってきた歴史があり、また金融分野では、通貨、決済は脱地方、東京中心、大手の金融機関中心、決済機関の集中の動きを加速させて、経済成長と相まって金融立国を果たして来た。ところが人口減少や少子高齢化の下で、その行き詰まりと地域経済社会の持続可能性が政治経済の課題になっている。そこにコロナ感染症を受けた新生活様式が、非接触、非都心、非東京での生活やビジネスを考える契機になっている。もとより通貨や証券は、効率よい安全な大規模な金融市場を中心とした価値移転だけがその役割ではなく、生活や経済活動の道具である。価値移転は、それ自体が独立してあるわけではなく、主体や原因が関与しているが、関与している内容の情報を切り離して無記名、転々流通、抗弁遮断など効率が追求され、法やコンピューター技術はこれを支えてきた。しかし、最近ではマネロン、個人情報保護など通貨や証券の価値移転を制約する動きも中央集権、グローバリゼーションが極まった後に論点化している。

通貨や証券は、元々は色のついたもの

自律分散社会志向と BC 技術による通貨、証券の展開ー未来は決まっていない

BC 技術も道具としての通貨や証券を機能させるための 1 つの技術だから、生活や経済活動の態様変化の影響は免れない。BC 技術は、自律分散社会と相性がよく、その社会のニーズに合った通貨、証券の発行流通形態が構築できると考える。通貨や証券の価値移転の技術が変革すれば、資金貸借、貸借の信用、金利といった基本的概念に変化はないとしても、これまでその担い手であった中央銀行を含む銀行や証券など金融機関のサービス内容や組織体の経営のあり方に影響があろう。勿論、自律分散社会に世界中がなるとは限らないし、その時間軸も決まっていない。ただ、そうした方向を市民、消費者、非金融機関企業、中でも中小企業や自治体、NPO など従来金融市場に直接アクセスできなかった主体が持ちうる技術ができ、その方向を望めばいろいろ工夫のできる時が来ているという認識は、中央銀行も含めて既存の金融機関にとって極めて重要なことだと考える。未来は決まっていない、不易と流行の当てはめについての意識を変えたものだけが生き残るのである。

以上