国際取引法学会第５号
目　次

2. 有価証券の電子化のためのブロックチェーン利用の法的課題

― 船荷証券と UNCITRAL モデル法に着目して ―

Legal Issues Arising From the Use of Blockchains for the Dematerialization of Negotiable Instruments

― with a Particular Focus on Bills of Lading and the UNCITRAL Model Law ―

高橋宏司（同志社大学司法研究科教授）

Koji Takahashi *, Doshisha University Law School, Professor

Abstract

This article considers the legal challenges which will be encountered when blockchains are used to dematerialize negotiable instruments such as bills of lading. The digitization of negotiable instruments yields a lot of benefits to the society but has been hampered by various technological and legal obstacles. On the technological side, this article examines the advantages and drawbacks of the blockchain as a tool for dematerializing negotiable instruments. On the legal side, there is a lot of uncertainty over the permissibility of, and the legal requisites for, dematerializing negotiable instruments. To improve certainty, the UNCITRAL created the Model Law on Electronic Transferable Records in 2017. The Model Law lays down the attributes which an electronic record needs to possess before it is deemed to be functionally equivalent to the corresponding "transferable instrument," a term broadly synonymous with "negotiable instrument." Thus, the electronic record must, by virtue of a reliable method, be identifiable (which implies the consistency of the record) and amenable to exclusive control. This article considers whether blockchain-based electronic records have these attributes. Among such attributes, the reliability of the method poses a particular challenge to the current law since the latter is not accustomed to evaluate the reliability of blockchains. Prior to the emergence of the blockchain technology, electronic records could only be maintained by an administrator of the database. It follows that under the conventional approach, the reliability of the method would be ensured through the regulation and oversight of the administrator. The blockchain, on the other hand, is a trustless technology which is founded on the notion that a system dispensing with the need for administrators is reliable for the very reason that it is distrustful. Whether the law is ready to embrace this notion will be tested if the society is to harness the full potential of the blockchain.

1. はじめに

本稿では、有価証券の電子化のメリットを踏まえ、電子化の手段としてのブロックチェーン（blockchain）の長所と短所を検討し、次に、法的課題として、有価証券の電子化の要件をブロックチェーンを用いた分散台帳（distributed ledgers）が備えることができるかを考察する。検討の際には、有価証券の一つの典型例として船荷証券に着目し、国連国際商取引法委員会（UNCITRAL）において2017年に採択された「譲渡性電子記録に関するモデル法」[1]（Model Law on Electronic Transferable Records（以下「モデル法」と略称））を素材とする。

2. 電子化のメリットと障害

有価証券を電子化すると、紙媒体を扱う費用の節減といったすべての有価証券に共通のメリットのほか、それぞれの有価証券に特有のメリットがありうる。船荷証券の場合、先に船が仕向港に到着し、船荷証券と引き換えられることなく運送品が仮渡しや保証渡しされる状況が頻発しているという、いわゆる「船荷証券の危機」を克服するのに有効である。

船荷証券の電子化の試みは過去30年以上にわたって続けられている。しかしながら、いまだ電子船荷証券が普及しているとは言い難い。普及を妨げている理由について、様々な指摘がなされている。例えば、電子化の最初の試みであったSeaDocsプロジェクトが頓挫した理由として、チェース・マンハッタン銀行の管理下にあるサーバに取引情報が集積することに対して、他の銀行が大きな懸念をもったことが挙げられている[2]。その後も電子化の試みは続けられたが、UNCTADのアンケート調査によると、取引相手等の電子化に対する準備不足や、法的枠組みの不明確さ・不十分さが電子化の主要な障害として回答されており、取引情報の機密保持に対する懸念などもそれに続いている[3]。では、電子化の手段としてブロックチェーンを利用することで、これらの障害が克服ないし軽減されることになるであろうか。以下では、まず、ブロックチェーンの意義と種類を確認した後に、この点を検討する。

3. ブロックチェーンの意義と種類

ブロックチェーンには、数多の種類があり、定義は容易でない。しかし、最広義では、「一定量の取引履歴をブロックとしてまとめ、それを鎖状につなげた構造をとる追記専用の電子記録簿である」と言えるであろう。ブロックチェーンは、ネットワーク上に分散的に保持される台帳（分散台帳）の間で記録を同期させる手段として有効なデータ構造であるので、分散台帳において利用されている[4]。これに対して、従来から存在するサーバ＝クライアント型の電子記録システムにおいては、管理者が存在し、その一存でサーバ（集中管理サーバ）の記録の変更が可能であり、管理者の許可を得た者のみが利用権限を有す

る。

ブロックチェーンを用いた分散台帳が初めて世に誕生したのは、約10年前にビットコインが発明された時である。ビットコインの分散台帳は、その設計思想に則り、管理者を有さず、あらゆる者の利用（閲覧と書込み）に開放されている。その後、特定の運営者[5]が存在し、利用にその者の許可が必要とされる分散台帳が開発され、許可制（permissioned）ブロックチェーンと呼ばれるようになった。そして、これとは対照的に、あらゆる者の利用に開放されているものは非許可制（permissionless）ブロックチェーンと呼ばれるようになった[6]。

ブロックチェーンの改竄耐性や攻撃耐性は、ブロック追加手順（アルゴリズム）に依存するが、これまでに開発されたブロックチェーンが採用するアルゴリズムは様々である。許可制ブロックチェーンは、運営者の許可を得た複数の処理者によって、分散的にブロック追加の合意形成がなされる。これに対して、非許可制ブロックチェーンは、一般に誰もがブロック追加の合意形成に参加できるが、中には、ブロック追加権限の分散度が低い設計のものもある。例えば、トークン保有者の投票で選ばれた複数の処理者の検証と多数決によってブロックが追加されるというアルゴリズムである。このような手順によれば、ブロック追加権限の分散度は後退するが、投票を定期的に繰り返して実施することで、ブロック追加権限を有する者の固定化を避ける設計も可能である。

4. ブロックチェーン利用のメリットと課題

ブロックチェーン上では、様々な客体をトークンとして表現することができる。ブロックチェーンは、「インターネット以来の革命」と言われることがあるが、それは、ブロックチェーンが特定の第三者を介在させることなく、オンライン上での価値の移転を史上初めて可能にした点が画期的だからである。ブロックチェーン上には、非代替トークン（non fungible token）と呼ばれる1つ1つが区別できるトークンも発行でき、それによって、船荷証券等の個別的な客体を表現することもできる。

前述したとおり、UNCTADのアンケート調査では、船荷証券の電子化を妨げる原因として、取引相手等の準備不足を挙げる回答が多かった。従来、船荷証券の電子化プロジェクトは、いずれもサーバ＝クライアント型の電子記録システムによるものであったが、それは、サーバの利用が契約メンバーに限られた閉鎖的なシステムであるため、取引関係者が同じシステムのメンバーになっていないかぎり、電子船荷証券の利用ができない。この障害は、いずれの者も利用が可能な非許可制ブロックチェーンを使えば、回避できる[7]。

サーバ＝クライアント型の船荷証券電子化プロジェクトが普及しないもう一つの理由は、SeaDocsプロジェクトについて見た通り、管理者に取引情報が集積することへの懸念である。この懸念は、ブロックチェーンを使えば、管理者が存在せず、記録が分散管理されるため、緩和されるかもしれない。しかし、管理の分散と機密保持の確保がトレードオフの関係に立つことにも注意が必要である。すなわち、分散台帳では、情報が特定の管理者に集中しない代わりに、各参加者に共有されることになる。先に見たとおり、UNCTADのアンケート調査では、電子化を妨げる要因として、比較的少数ではあったが、取引情報の機密保持に対する懸念を挙げる回答があった。ブロックチェーン上の取引は仮名（pseudonym）で行うことができるが、取引の流れはブロックチェーン上に記録されるので、ブロックチェーン外の情報と照らし合わせることによって、取引当事者の特定がなされる可能性がある。確かに、船荷証券の原文は、ブロックチェーンの外でやりとりし、そのハッシュ値のみをブロックチェーン上に記録することも可能であるし、また、様々な秘匿技術も考案されている。しかし、分散台帳である以上、集中管理サーバと異なり、構造上、記録が多人数の閲覧に供されることになるのは避けられない[8]。したがって、ブロックチェーンを利用した分散台帳が電子船荷証券のプラットフォームとして選択されることになるかを左右する要因として、船荷証券関係者の求めるレベルの機密保持が技術上可能であるか、そして、当該レベルでの機密保持が可能なことを前提に、情報を分散的に共有する方が、集中管理サーバの管理者にすべての情報を委ねるよりも関係者の選好度が高いかが挙げられよう。

5. 法的問題の所在

前述したUNCTADのアンケート結果では、法的枠組みが不明確・不十分であることも、電子化を妨げる主要な原因の一つとされている。これは、電子記録として表現された船荷証券が広く各国で「船荷証券」として法的に承認される確実性がないことを指しているものと考えられる。次の仮想事例を考えてみたい。

AがBとの間で動産XをBに売り渡す契約を締結し、運送書類として電子船荷証券を引き渡すことに合意した。Aは、この契約を履行するため、CにXの運送を委託する契約をCとの間で締結し、Cは、電子船荷証券を発行することに合意した。Aは、Cから発行された電子船荷証券をBに引き渡した。ところが、その後、Aは、DにXを売り渡す契約を締結した。Bは、Dに対して、Xの所有権を対抗できるか。なお、以下の日本法の規定が適用されるものと仮定する。

> 民法178条（動産に関する物権の譲渡の対抗要件）動産に関する物権の譲渡は、その動産の引渡しがなければ、第三者に対抗することができない。
>
> 商法763条（船荷証券の引渡しの効力）船荷証券により運送品を受け取ることができる者に船荷証券を引き渡したときは、その引渡しは、運送品について行使する権利の取得に関しては、運送品の引渡しと同一の効力を有する。

そもそも紙媒体により船荷証券として作成されたものであっても、「船荷証券」として法的に承認される要件（日本法では、商法758条所定の要件）を備えなければ、単なる紙切れにすぎず、商法763条に規定するような効力を生み出さない。同様に、電子記録も、A、B、C間でそれを船荷証券として扱うことに合意しただけでは、法的に「船荷証券」として承認されない限り、合意の当事者でないDとの関係では何らの効力も生まない。

では、電子記録は、どのような要件を充たせば、法的に「船荷証券」として承認されるか。また、その引渡しは、どのような要件を充たせば、法的に「引渡し」として承認されるか。これらの点について、ほとんどの国の法は不明確である[9]。日本法の下でも、海上

運送状については、電磁的方法による提供に関して定めがある（商法770条3項）のに対して、船荷証券については、電子化の許否と要件に関して定めがない。船荷証券電子化のこのような法的障害は、電子記録システムを集中管理サーバから分散台帳に変えることによって回避できるものではない。法的枠組みの明確化は、電子記録システムの種類にかかわらない共通の課題である。

6. モデル法の目的と適用対象

この法的課題を解決するために立法する場合に参考となるのが前記のモデル法である。モデル法の目的は、端的に言うと、有価証券と電子の世界を架橋することにある。そのために、「譲渡性書類・証券（transferable document or instrument）」を電子記録によって代替するために、電子記録が備えなければならない要件を定める。「譲渡性書類・証券」とは、その定義（第2条）[10]によると、債権を表章する書類で、それによって当該債権の移転および行使が可能であるものであり、概ね有価証券に相当する。船荷証券は、その一例である。ビットコインのような仮想通貨は、債権を表章するものではないので、モデル法の適用対象外である。本稿では、仮想通貨のブロックチェーンにも言及しているが、それは、ブロックチェーンの設計例として比較的よく知られているからに過ぎない。

仮に日本でモデル法を参考にした立法をするならば、改正後民法の第3編「債権」の第1章「総則」に新設される第七節「有価証券」が、有価証券に関する通則的な規定群を一本化して置くので、その中に規定を入れ込むのが適当であろう。ただし、わが国では、電子記録債権法が制定されているので、手形については、電子化は特に必要がないとの立場に立ち、船荷証券についてのみ立法的手当てをするならば、商法の第三編「海商」の第三章「海上物品運送に関する特則」の中の第三節「船荷証券等」に規定を入れ込むこととなろう。いずれにせよ、有価証券の電子化の立法をするならば、モデル法自体を採用するか否かにかかわらず、それと大差ない要件を立てることとなると考えられる。そこで、以下では、モデル法の要件に即して検討する。

7. 技術中立性と機能的等価性

モデル法は、技術中立性（technology neutrality）の原則を採用しており、特定の技術の利用を前提としていないので、従来型の集中管理サーバは当然のこと、ブロックチェーンもその適用範囲から除外されていない。

しかし、「譲渡性書類・証券」と機能的等価性（functional equivalence）を有する電子記録のみが法的にそれらと同視される。モデル法の第10条および第11条[11]によると、機能的代替性が認められるには、①電子記録の「譲渡性電子記録」としての特定可能性があること、②その排他的支配可能性があること、および③それを実現する方法が信頼可能であることが要件となっている。これらの要件は、電子化の手段として、従来型の集中管理サーバが用いられた場合にも当然適用されるが、本稿のテーマに即して、以下では、ブロックチェーン上の電子記録がこれらの三要件を充たすかを順に検討する。

8. 要件①「譲渡性電子記録」の特定可能性

有価証券は、原本の占有とその引渡しを通じて、それが表章する同一の債権につき、複数の者から権利主張がなされることを防いでいる。これを電子的環境で実現するためには、同一の債権を表章する異なる電子記録が二つ以上存在してはならないことになる。ところが、原本（original）を情報が最初に固定された媒体として定義すると、電子の世界で受取人が受け取るデータ・メッセージは、いずれもコピーである[12]。また、コピーの作成がシステム設計上必要となることもある。特に、ブロックチェーンは、分散台帳であるので、多数の参加者が分散的にコピーを保持する。

先に見たように、モデル法は、ある電子記録が有価証券と機能的に等価であるためには、当該電子記録が「譲渡性電子記録」として特定されなければならないという要件を立てている（第10条（1）（b）（i））。これは、電子記録のコピーの有無に着目するのではなく、その一意性（「一貫性」とも言う）が確保されているかを問う要件であると言えよう。

集中管理サーバでは、管理者がサーバの記録を専権的に制御するので、電子記録の一意性の確保が可能である。他方、分散台帳では、電子記録が複数の参加者に分散的に保持されている。それでも、許可制ブロックチェーンの場合、ブロック追加権限を有する者が特定の者に限定されているので、一意性の確保は不可能でない。これに対して、非許可制ブロックチェーンの場合には、不特定多数の者がブロック追加権限を有するため、その一意性を確保することには、元来、かなりの困難があるはずである。

非許可制ブロックチェーンのアルゴリズムは一様でないが、その原型であるPoW（Proof of Work）と呼ばれるものは、分散台帳の自律的な同期を可能にした[13]。それは、ビットコインの価値を担保する革新的なアルゴリズムであるが、果たして、それによって一意性が確保されたとまで言いうるであろうか。注意すべきは、PoWによる同期のファイナリティは確率的なものでしかないということである。ファイナリティの概念を厳格に解すると、それが欠如しているとも言えよう。このアルゴリズムでは、演算能力の競争を通じてブロックが追加されていくが、その過程で、チェーンに分岐が生ずることがあり、その場合に、短い方のチェーンは巻き戻されて無効と扱われてしまう。分岐は、演算結果がネットワーク上を伝播し、各参加者に到達するのにタイムラグが生ずることから、平常時にも起こりうるし、後述するように、チェーンへの攻撃によっても起こりうる。ファイナリティの確率は、ブロックの確認数が増えるにつれて指数関数的に上昇していく。そこで、契約の履行手段としてブロックチェーン上のトークンを用いる場合には、両当事者の納得する確率に到達する確認数を合意しておくことができる。例えば、売買の対価としてビットコインを引き渡すことを合意した場合、6ブロックの確認を経ることによってビットコインの引渡しがなされたとみなす合意が可能である。仮に、7ブロック目以降においてチェーンが巻き戻された場合には、不当利得にもとづく返還請求などで債権債務関係を清算することになる。ところが、有価証券の引渡しの効力は、特定の当事者間の債権債務関係に限定された問題ではない。例えば、前記の仮想事例において、電子船荷証券の発行にブロックチェーンを用いる場合、そのアルゴリズムにファイナリティがなければ、電子

船荷証券がBに引き渡された記録が破棄されることが起こりうる。AとBの関係は、両者間の契約とそれを巡る債権債務関係の清算で解決するが、BとDの関係は契約関係ではなく、船荷証券の引渡しの記録が破棄されてしまうと、Bは、Dに対して、Xの所有権を対抗できなくなり、船荷証券の物権的効力が否定されることになる。したがって、ブロックチェーン上の「譲渡性電子記録」の特定可能性は、確率的なファイナリティしか有さないPoWのようなアルゴリズムを当該ブロックチェーンが採用する場合には、否定せざるをえないであろう。

非許可制ブロックチェーンのアルゴリズムにも、1ブロックごとに即時に同期のファイナリティが得られるものもある。例えば、トークン保有者の投票で選ばれた複数の者の検証と多数決を通じてブロックがチェーンに追加されて行くというアルゴリズムである。このように確定的なファイナリティが得られるアルゴリズムであれば、チェーンの分岐が生じず、電子記録の一意性は確保される。

9. 要件② 排他的支配可能性

有価証券は、原本の占有とその引渡しを通じて、それが表章する同一の債権につき複数の者から権利主張がなされることを防いでいる。しかし、電子記録は、有体物ではないので、占有ができない。そこで、先に見たように、モデル法は、ある電子記録が有価証券と機能的に等価であるためには、それに対する排他的支配可能性が認められなければならないとしている（第10条（1）（b）（ii）、第11条）。では、ブロックチェーン上の電子記録に排他的支配可能性が認められるであろうか。まず、私見を述べた後、東京地裁の説示を検討する。

a. 私　見

従来型の集中管理サーバでは、その管理者によって権限を認められた者のみが、電子記録の変更を指示することができるので、電子記録に排他的支配可能性が認められると言えよう。

ブロックチェーンでは、あるアドレスに格納されているトークンは、そのアドレスに対応する秘密鍵を用いなければ引き出すことができないようにスクリプトを書くことができ、その場合、当該トークンは秘密鍵を把握する者の排他的な支配に服する。実際、そのような実装が典型的である。したがって、ブロックチェーン上の電子記録には排他的支配可能性が認められると言ってよいように思われる。なお、数多ある有象無象のブロックチェーンには、ブロック生成が停滞し、トークンに経済的価値がないものも多いが、それは次に検討する要件③の信頼可能性に関係するとしても、排他的支配可能性の有無とは無関係と言えよう。

b. 東京地判

東京地裁は、所有権にもとづくビットコインの引渡しが請求された事件において、ビットコインについて、「所有権の客体となるために必要な…排他的支配可能性を有するとは

認められない。」と判断した[14]。所有権の客体となる要件としての排他的支配可能性と、モデル法の下での排他的支配可能性は同義である必然性はないが、概念の類似性は否定できないから、前者について否定する判断が出された以上は、その根拠を精査する必要がある。

同判決は、「ビットコインの仕組み、それに基づく特定のビットコインアドレスを作成し、その秘密鍵を管理する者が当該アドレスにおいてビットコインの残量を有していることの意味に照らせば、ビットコインアドレスの秘密鍵の管理者が、当該アドレスにおいて当該残量のビットコインを排他的に支配しているとは認められない。」と説示し、(1) ビットコインの仕組みと (2) アドレスにおいてビットコインの残量を有していることの意味をその判断の根拠とした。そこで、以下では、この二つの根拠を順に検討する。

i. ビットコインの仕組み

一つ目の根拠とされたビットコインの仕組みについて、東京地裁は、次のように説明している。「一定数のビットコインをあるビットコインアドレス（口座A）から他のビットコインアドレス（口座B）に送付するという結果を生じさせるには、…①…、②送付元の口座Aの秘密鍵を管理・把握する参加者が、作成したトランザクションを他のネットワーク参加者…に送信する、③トランザクションを受信した参加者が、当該トランザクションについて、…検証する、④…検証した参加者は、当該トランザクションを他の参加者に対し…転送し、…当該トランザクションが…広く拡散される、⑤拡散されたトランザクションがマイニングの対象となり、マイニングされることによってブロックチェーンに記録されること、が必要である」。そして、この説明を踏まえて、「口座Aから口座Bへのビットコインの送付は、口座Aから口座Bに『送付されるビットコインを表象する電磁的記録』の送付により行われるのではなく、その実現には、送付の当事者以外の関与が必要である」と指摘している。

この指摘は正しいが、それが排他的支配可能性を否定する根拠となり得るかは、疑問である。この理屈によるならば、銀行の集中管理サーバに記録されている預金についても、その移転記録の実現には、サーバ管理者である銀行の関与が必要であることを根拠として、預金の排他的支配可能性が否定されてしまい、預金の帰属について行われてきた議論の前提が成り立たなくなるように思われる。

ii. アドレスにおいてビットコインの残量を有していることの意味

東京地裁は、ビットコインについて、排他的支配可能性を否定する判断のもう一つの根拠として、アドレスにおいてビットコインの残量を有していることの意味を挙げた。この意味について、同判決は、「特定の参加者が作成し、管理するビットコインアドレスにおけるビットコインの有高（残量）は、ブロックチェーン上に記録されている同アドレスと関係するビットコインの全取引を差引演算した結果算出される数量であり、当該ビットコインアドレスに、有高に相当するビットコイン自体を表象する電磁的記録は存在しない。」と指摘している。

この指摘のとおり、ビットコインのブロックチェーン上に存在するのはアドレス間の

個々の取引履歴だけである。これに対して、イーサリアムなどアカウントベースのブロックチェーンには、全体の取引履歴を反映するstate（現状）が記録されており、銀行口座のように、アカウントと最新の残高を示す記録があるので、説示の指摘は当てはまらない。ビットコインのブロックチェーンのように、個々の取引履歴が記録されているにすぎないものであっても、差引演算によって、アドレス毎の有高（残量）を算出し、UTXO（unspent transaction output: 未使用トランザクションアウトプット）として観念できる以上、それに対する排他的支配可能性を認めることは可能であると考える。

10. 要件③ 信頼可能性

先にみたように、モデル法は、電子記録に有価証券との機能的代替性が認められるためには、信頼できる方法によって、当該電子記録が「譲渡性電子記録」として特定でき、その排他的支配ができなければならないとしている（第10条（1）（b））。

a. モデル法の規定

信頼可能性（reliability）の判断基準について、モデル法は、「当該方法が使用される機能を果たすために相当な程度の信頼可能性」を求め、第12条に次のように規定している（抄。私訳）[15]。

> 第12条　一般的信頼可能性基準
> 第…10条、11条…の規定する方法は、次のいずれかでなければならない。
> (a)　当該方法が使用される機能を果たすために相当な程度の信頼可能性があること。信頼可能性は、次の諸点を含め、すべての関連する状況に照らして判断される。
> (i)　信頼可能性の判断に関係するオペレーション・ルール
> (ii)　データの一貫性
> (iii)　システムへの無許可のアクセスや利用を防ぐ性能
> (iv)　ハードウェアおよびソフトウェアの安全性
> (v)　独立機関による監査の頻度と程度
> (vi)　監督機関、認定機関、自主的制度による当該方法の信頼可能性に関する宣言の存在
> (vii)　産業規格
> (b)　それ自体として、あるいは他の証拠と合わせて、その機能を果たしたことが証されていること。

前記の仮想事例において、Dが当該電子船荷証券の発行および引渡しに用いられた方法の信頼可能性を争ったとすると、裁判所はこの規定に則ってその信頼可能性の有無を判断することになる。しかし、用いられた方法の信頼可能性の有無について、紛争になってから裁判所等の裁定機関によって、事後的に判断されるしかないとすると、予測可能性に欠けるため、電子的方法の利用が敬遠されてしまう。これに対して、信頼可能性が認められる方法が事前に指定されていれば、安心してその方法を利用できるようになる。

モデル法12条の（b）項は過去形で表現されており、事後的判断にのみ適用される。しかし、（a）項の列挙事由には、「監督機関、認定機関、自主的制度による当該方法の信頼可能性に関する宣言の存在」（vi号）があり、事前指定も可能であることを示唆している。他の（a）号列挙事由は、事前指定の際にも考慮要素となるであろう。

b. 事前指定に関する現行法のアプローチ

モデル法は、事前指定について、これ以上具体的な規定を置いていないが、モデル法に依拠した法整備の最初の事例であるバーレーンの譲渡性電子記録法[16]（Law No. 55 of 2018 with Respect to Electronic Transferable Records）は、事前指定の手続、要件、効果を定める規定を置いている。

同法によると、電子記録システムの運営者の申請にもとづき、権限当局は、当該運営者を「指定運営者」として指定することができる（第15条[17]1項）。指定の要件や手続は、所轄当局の制定する規則（regulation）の定めるところによる（同条2項）。指定運営者は、権限当局の監督や権限当局が規則において定める検査に服することになる（同条4項）。指定運営者に用いられる方法の信頼可能性は、法的手続の下では、異なる証拠が提出されないかぎり推定され（第8条2項[18]）、これが指定を受けるメリットであると考えられる。反面、指定運営者は、自らが運営する譲渡性電子記録に依拠することにより他人に損害が発生した場合、過失の推定により、加重された民事責任に服する（第17条[19]）。

このように、バーレーン法は、電子記録システムの信頼性をその運営者の統制を通して担保している。これは、法が電子記録システムの信頼可能性を要件としている場合に、その法目的を問わず、各国の現行法が採用している標準的なアプローチであろう。例えば、日本の電子記録債権法や社債、株式等の振替に関する法律にも同様のアプローチが見られる。電子記録債権法は、電子記録債権という金銭債権を創設した。これは手形とは異なり、電子的環境においてのみ存在する新しい類型の権利であるから、手形の電子化のためにモデル法を国内法化した形とは様相が異なる。しかし、電子記録システムの信頼性を担保する重要性は同法の下でも変わらない。同法は、そのために、電子債権記録機関に行政的監督を及ぼし（第73条1項）、過失の証明責任を転換し、加重された民事責任を課している（第11条）。また、電子債権記録業者としての指定を申請する者に対して、人的構成、財産的基礎および組織的ガバナンスに関する要件を定めている（第51条1項。特に第1、6、7号参照）。電子記録債権業者や社債、株式等の振替に関する法律における振替業者が、一定の機関を置く株式会社でなければならないとされている（電子記録債権法51条1項1号、振替法3条）のは、これらの運営者には、しっかりしたガバナンスを求める趣旨である[20]。

c. ブロックチェーンの信頼可能性判断

i. 事前指定に関する現行法のアプローチへの適合性

電子記録システムの運営者の統制を通して、その信頼性を担保しようとする現行法のアプローチは、管理者の存在する従来型の集中管理サーバに適合的である。しかし、非許可制ブロックチェーンには、管理者・運営者が存在しないため、このアプローチをとりえない。バーレーンの譲渡性電子記録法の下では、権限当局が「指定運営者」を指定しように

も、そもそも指定申請をする者が存在しないことになる。これに対して、許可制ブロックチェーンの場合は、運営者が存在するため、このアプローチに適合的である[21)]。しかし、法が運営者に対して民事責任を課すだけでなく、電子記録の訂正義務まで課す（電子記録債権法第10条参照）ならば、記録の書換え権限を単独で掌握する管理者が存在しなければならず、許可制ブロックチェーンであっても、通常は、それを可能とする設計にはなっていないと考えられる。なぜなら、そのような管理者を置くのならば、集中管理サーバを利用すればよく、そもそも分散台帳を利用する根本的な趣旨に反するからである。

このように、現行法のアプローチの下では、信頼可能性の認められる電子記録システムを事前指定する枠組みにブロックチェーンを用いた分散台帳を取り込むには、困難が生じうる。

ii. トラストレス（trustless）の意味

では、ブロックチェーンは、本来的に、信頼可能性を認めることが困難なシステムなのであろうか。ブロックチェーンは、「トラストレス（trustless）」な仕組みであるとよく言われる。オックスフォード英語辞典（第3版、2015年）には、trustlessという言葉に二つの意味が掲載されている。一つは、「信頼を置かない（distrustful）」という意味であり、もう一つは、「信頼に値しない（unreliable, untrustworthy）」という意味である。「ブロックチェーンはトラストレスな仕組みである」と言われるときは、第一の意味で「ブロックチェーンは、仲介者に信頼を置かない仕組みである」と言っているのであって、第二の意味で「ブロックチェーンは信頼に値しない仕組みである」と言っているわけではない。むしろ、「仲介者に信頼を置かない」からこそ「信頼に値する仕組みである」というのがブロックチェーンの根本にある思想である。

管理者の存在する電子記録は、その管理者によって、またはその者を通じた攻撃によって、検閲や改竄を受けるおそれがある。管理者の統制を通して電子記録システムの信頼性を担保しようとしている現行法のアプローチは、いわば管理者に対して不信を抱きつつも、管理者に信頼を置かざるを得ないジレンマを抱えたものであると見ることもできよう。従来は、管理者不在の電子記録システムが構築できるとはおよそ考えられなかったため、このジレンマは意識されることすらなかった。ところが、ブロックチェーン技術の誕生によって、仲介者を排して、不特定多数の者の間で自律的に機能する電子記録システムが構築できるようになった。しかも、それにより、集中管理サーバよりも優れた改竄耐性、改竄検出性、攻撃耐性、障害耐性を実現することも可能となった。

今後、ブロックチェーンの社会的受容を進めていくとすれば、法には次のようなパラダイム転換を受け入れるべきかの問いが投げかけられるであろう。すなわち、電子記録システムの信頼性は、その管理者の統制を通して担保するほかないという従来からの思考枠組みにとどまるのか、それとも、「仲介者に信頼を置かない」からこそ「信頼に値する仕組みである」というブロックチェーンの思想に門戸を開くかである。

iii. 紙媒体との対比

このパラダイム転換は、電子の世界では、コペルニクス的転回とも呼べる大転換である。しかし、実は紙媒体の世界においては、管理者不在のシステムに信頼可能性を認めることに目新しさはない。と言うのは、紙媒体の有価証券のやり取りは、仲介者に信頼を置かず、相対でなされるtrustlessな仕組みだからである。

管理者不在のシステムの信頼性は、その媒体の性質に依拠するほかない。単一の債権について、複数の者からの権利主張がなされることを防いでいる有価証券の機能は、専ら紙という媒体の性質に依存している。すなわち、複写と区別されるところの原本を観念でき、その物理的な占有が可能であるという性質である。ブロックチェーン上の有価証券は、ブロックチェーンの媒体としての性質に依存することになる。すなわち、先に検討したとおり、「譲渡性電子記録」の特定とその排他的支配が可能であるという性質である。

iv. アルゴリズムの信頼性評価

ところで、「仲介者に信頼を置かない」ことは、ブロックチェーンが「信頼に値する仕組みである」ための必要条件であるが、十分条件ではない。その信頼性の源泉は、アルゴリズムにある。ブロックチェーンは、参加者各人が利己的に行為したとしても機能するよう、プロトコル設計とインセンティブ設計を組み合わせた様々なアルゴリズムを採用している。しかし、その信頼性評価は容易ではない。なぜなら、プロトコル設計の堅牢性は、その評価に技術的な知識が必要であるだけでなく、その策定に関与する者の議論や技術革新等によって、時間変化しうるからである。また、インセンティブ設計の有効性も、マイニングの状況等の外部要因の影響を受けて時間変化しうるからである。

最後の点について、代表的なアルゴリズムであるPoW（Proof of Work）の場合を例に説明を試みたい。このアルゴリズムによって生成されるブロックチェーンには、前述したとおり、演算結果がネットワーク上を伝播するタイムラグを原因として分岐が生ずることがあるが、分岐は、「ブロック隠し持ち攻撃（Block Withholding Attack）」と呼ばれるチェーンに対する攻撃によっても生ずる。これは、演算力の大きい攻撃者がブロック追加作業を続けながら、それをネットワークに流さずに隠れて二重取引を行い、その後になって、密かに追加してきたブロックを一挙に流し、他のネットワーク参加者が紡いできたより短いチェーンを巻き戻させて利益を得るものである。この攻撃手法が可能であることは既知であったが、現実化しにくいと思われていた。ところが、ブロック追加に要する演算量が異なる多数の仮想通貨が誕生し、仮想通貨の交換が交換所を通じて容易になったという環境の変化により、攻撃を仕掛ける経済的なインセンティブが高まった。その結果、よく知られた仮想通貨（モナコイン、ビットコイン・ゴールド、イーサリアム・クラシックなど）のブロックチェーンに対する攻撃が功を奏する事例が生じた。

v. 脆弱性との共生

ブロックチェーンの様々なアルゴリズムは一長一短であり、PoW以外のものでも、脆弱性が皆無であるものは存在しない。しかし、翻って見ると、紙媒体の有価証券にも脆弱性は存在する。船荷証券では複本を発行する実務が根強く、他の有価証券でも高性能複写

機によって原本に酷似する複写が作成され、流通する可能性がある[22)]。船荷証券の複本発行の実務は、送付中に紛失や遅延が起こり得るという紙媒体の性質から派生したものであるから、高性能複写機による複写作成と同様、紙という媒体の性質に起因する脆弱性である。にもかかわらず、法は紙媒体の信頼可能性を一般的には認めた上で、偽造・変造等の問題に対処している。したがって、ブロックチェーンという媒体についても、信頼可能性を認める要件として、脆弱性が皆無であることを求めるのは行き過ぎであろう。

ある程度の脆弱性とは共生せざるをえず、モデル法が要求しているとおり、「機能を果たすために相当な程度の信頼可能性」（第12条（a））の有無を適時に判断することが求められると考えるべきであろう。紛争発生後の事後的判断では、取引時に遡って、その時点での信頼性評価を行うのが妥当であろう。事前指定については、電子記録システムの管理者・運営者の統制を通して、その信頼性を担保する現行法の標準的アプローチだけではなく、運営者の申請を要求せず、アルゴリズムに着目して、安定的に機能しているブロックチェーンを信頼可能性あるものとして指定するアプローチの可否も模索すべきであろう。その場合の信頼性評価は、判断時のものとなるが、前述したとおり、信頼性は時間変化しうるので、機動性のある見直しも必要であろう。プロトコル設計の堅牢性評価には、高度な技術的知識も必須であるので、指定の主体は、行政庁である必然性はなく、むしろ専門的かつ柔軟性ある判断が可能な業界団体に委ねる方が妥当かもしれない。

11. おわりに

「インターネット以来の革命」と言われることがあるにもかかわらず、ブロックチェーンは、その誕生後10年を経た現在もまだユースケースを模索している。ビットコインに代表される仮想通貨は、価値の貯蔵手段としては一定の役割を担っているが、支払手段としては、技術的にも改良の余地があり、法的にはマネーロンダリング規制の重しがかかる。ICOは、世界中から円滑に資金調達する手段として近年隆盛を見たが、詐欺事例が横行し、各国で証券規制が強められている。本稿で検討したブロックチェーン上の有価証券は「インターネット以来の革命」の一つの柱になりうると思われ、船荷証券、株券、社債券などで実務が動こうとしているが、技術的には、機密保持の要請とどう折り合いを付けるかなどの課題があり、法的にもそれらが有価証券として承認されなければ、「革命」は実現しない。

法的承認のハードルは、モデル法の要件に即して言えば、①電子記録の「譲渡性電子記録」としての特定可能性があること、②その排他的支配可能性があること、③それを実現する方法が信頼可能であることのいずれの要件についても克服すべき理論的課題がある。特に、信頼可能性のある電子記録システムを事前指定する際に、システムの管理者・運営者の統制可能性を前提とする現行法の標準的アプローチには、運営者の存在しない非許可制ブロックチェーンは親和性がない。法が電子記録システムの管理者に記録の訂正義務まで課すならば、許可制ブロックチェーンであっても、通常、その要件を満たすことはできない。今後、ブロックチェーンの社会的受容を進めていくならば、事後的に信頼可能性があったかを判断する局面も含めて、「仲介者に信頼を置かない」からこそ「信頼に値する

仕組みである」というブロックチェーンの思想に法がどこまで門戸を開くことができるかが問われていくと思われる。

注

＊　本稿は、国際取引法学会・UNCITRAL 共催シンポジウム「UNCITRAL モデル法と仮想通貨・ブロックチェーン」（第5回国際取引法学会全国大会（2019年3月16日）於：早稲田大学）における筆者の報告をもとに作成した。報告の場を設定していただいた久保田隆教授を初めとする学会関係者に御礼を申し上げたい。

1)　「電子的移転可能記録モデル法」と訳されることも多いが、記録自体が電子的に移転するわけではなく、電子記録が譲渡されたように観念できる状態が作出されるにすぎない。そこで、「譲渡性電子記録に関するモデル法」とでも呼ぶのが誤解を招きにくく、かつ英文タイトルからも大きく乖離しないのではないかと思われる。

2)　Boris Kozolchyk, 'Evolution and Present State of the Ocean Bill of Lading from a Banking Law Perspective' (1992) 23 J Mar L & Com 161, 228.

3)　UNCTAD, "The Use of Transport Documents in International Trade" (2003) (UNCTAD/SDTE/TLB/2003/3) para. 79 は、アンケート調査の結果を次の表にまとめている。

Obstacles to the use of electronic alternatives (more than one answer possible)	Responses (% of respondents)
Infrastructure/market/trading partners not yet ready	51
Legal framework is not clear enough or is not adequate	44
Electronic equivalents are not sufficiently secure	25
Technology and/or switch to electronic environment is too costly	12
Confidentiality concerns	10
Other reasons	2

4)　なお、分散台帳には、ブロックチェーンのデータ構造をとらないものもある。

5)　分散台帳では、集中管理サーバとは異なり、単独の者の一存による記録の書換えはできないため、本稿では、「管理者」ではなく「運営者」という言葉を用いる。

6)　閲覧と書込みを区別し、閲覧が開放されているか否かの基準により、パブリック・ブロックチェーンとプライベート・ブロックチェーンに分け、書込み権限を有する者が許可を得た者に限定されているか否かの基準により、許可制ブロックチェーンと非許可制ブロックチェーンに分ける分類法も存在する（Garrick Hileman & Michel Rauchs, "Global Blockchain Benchmarking Study" (2017) Cambridge Centre for Alternative Finance p.20）。パブリック・ブロックチェーンであっても、閲覧はあらゆる者に開放しつつ、特定の運営者が存在し、書込みはその者の許可を得た者に限られる形態（許可制ブロックチェーン）も観念しうるからである。本稿では、そのようなブロックチェーンは、書込み権限に着目し、許可制ブロックチェーンに含めて論じる。

7)　拙稿 "Blockchain Technology and Electronic Bills of Lading" (2016) 22 Journal of International Maritime Law pp.202, 205. この論文は、許可制ブロックチェーンの開発が盛んになり、世間の耳目を集める以前に執筆されたため、誰もが利用可能である点をブロックチェーン一般のメリットとして指摘した。

8)　Gideon Greenspan, "Blockchains vs centralized databases" (2016) (https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/)

9)　Clyde & Co., "The Legal Status of Electronic Bills of Lading: A Report for the ICC Banking Commission" (2018) p.7 参照。

10) 第２条は、定義規定であり、「譲渡性書類・証券」については、次のように定義している。

"Transferable document or instrument" means a document or instrument issued on paper that entitles the holder to claim the performance of the obligation indicated in the document or instrument and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.

なお、株券、社債券は、モデル法の適用対象外とされている（第１条（3））。

11) これらの条文は、第２章「機能的等価性に関する規定（Provisions on functional equivalence）」に置かれており、次のように規定している（抄）。

Article 10. Transferable documents or instruments

1. Where the law requires a transferable document or instrument, that requirement is met by an electronic record if:

(a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and

(b) A reliable method is used:

(i) To identify that electronic record as the electronic transferable record;

(ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and

(iii) To retain the integrity of that electronic record.

2. …

Article 11. Control

1. Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:

(a) To establish exclusive control of that electronic transferable record by a person; and

(b) To identify that person as the person in control.

2. Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

12) Guide to enactment for the UNCITRAL Model Law on Electronic Commerce, para 62.

13) その技術的説明は、Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" p.3 参照。

14) 東京地判平成 27 年 8 月 5 日、2015WLJPCA08058001.

15) 原文は次のとおり。

Article 12. General reliability standard

For the purposes of articles 9, 10, 11, 13, 16, 17 and 18, the method referred to shall be:

(a) As reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances, which may include:

(i) Any operational rules relevant to the assessment of reliability;

(ii) The assurance of data integrity;

(iii) The ability to prevent unauthorized access to and use of the system;

(iv) The security of hardware and software;

(v) The regularity and extent of audit by an independent body;

(vi) The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;

(vii) Any applicable industry standard; or

(b) Proven in fact to have fulfilled the function by itself or together with further evidence.

16) アラビア語の正文は、http://www.legalaffairs.gov.bh/Media/LegalPDF/K0217.pdf に掲載されている。筆者は、同法の起草を担当した Jameel Al Alawi 氏（バーレーン経済開発委員会（Economic Development Board）上級法律補佐官（Senior Legal Adviser））から英語訳文の提供を受け、自らのブログに掲載している（https://cryptocurrencylaw.blogspot.com/2019/03/bahraini-legislation-based-on-uncitral.html）。本稿の分析は、この英語訳文に依拠している。

17) 英語訳文（抄）は、以下のとおり。

Article（15）Accreditation of Operators

1. An operator which is incorporated in the Kingdom of Bahrain, or has a place of business in the Kingdom, may apply to the competent administrative agency to approve its accreditation as an accredited operator. …

2. The competent authority shall issue a regulation specifying the conditions and relevant criteria for the accreditation of any operation and procedure for submitting and processing the application ….

3. …

4. Accredited operators shall be subject to oversight by the competent administrative agency and such audit requirements as the competent authority may prescribe in a regulation.

5. …

6. …

18) 英語訳文（抄）は、以下のとおり。

Article（8）General Reliability Standard

1. …

2. …

In the course of any legal proceedings, the reliability of the method used by an accredited operator shall be presumed unless evidence to the contrary is adduced.

19) 英語訳文（抄）は、以下のとおり。

Article（17）Liability of Accredited Operators

1. … an operator shall be liable for damage caused to any person who reasonably relied on an electronic transferable record, for which the electronic transferable records management system of that operator has been used, where the damage is due to the operator's use of a method which does not satisfy the requirements provided under Articles 6 and 7 of this law, provided that the damage was the result of the operator's intention or negligence.

2. For the purposes of paragraph（1）, if the operator is accredited, it shall be presumed that the damage was due to the accredited operator's intention or negligence unless otherwise proven.

3. …

20) 始関正光＝高橋康文『一問一答　電子記録債権法』（2008 年、商事法務）183 頁、高橋康文＝尾崎輝宏『逐条解説　新社債、株式等振替法』（2006 年、金融財政事情研究会）49 頁。

21) 小出篤「『分散型台帳』の法的問題・序論――『ブロックチェーン』を契機として」江頭憲治郎先生古稀記念『企業法の進路』（2017 年）853 頁も同旨と解される。

22) 拙稿「高性能コピー、電子的書類呈示の時代における信用状呈示書類の『原本性』」国際商取引学会年報（2005 年）176 頁は、紙媒体が改竄に対してほとんど無防備であるのに対し、電子の世界では、より確実性の高い認証が可能であるため、紙の世界で複写技術の進歩によって原本の判別が困難になったという問題は、電子技術の進歩によって解決の路が開かれる可能性があると指摘している。