第１章　仮想通貨のファイナリティ

岩　原　紳　作

１　ファイナリティ概念

（１）総説

ファイナリティとは、一般に「決済が無条件かつ取消不能となり、最終的に完了した状態」と定義されている（嶋拓哉「資金決済におけるファイナリティ概念について――ファイナリティ概念の多義性を巡る法的検証」http://www.fsa.go.jp/frtc/nenpou/2006a/11.pdf　1 頁）。しかしその内容は多義的で、資金決済のファイナリティには、①当事者間完了性、②対第三者完了性、③資金決済完了性、④支払指図の撤回不能性、以上の 4 つの異なる意味があると指摘されてきた（古市峰子「現金、金銭に関する法的考察」金融研究 14 巻 4 号（1995 年）117～119 頁）。しかしファイナリティにはこれ以外にも色々なレベルでのファイナリティが存在し得る。当該決済システムの内部では決済が完了したものと扱われても、アメリカでは、仕向銀行が二重に振込指図を送信した場合（重複送信）等には、被仕向銀行の同意を条件に支払指図の撤回を認めているし（岩原紳作『電子決済と法』（有斐閣、2003 年）288 頁以下）、振込依頼人による誤振込に関するわが国の判例は、入金記帳後の受取人の権利を場合によっては否定する結果を導いているし（最判平成 15・3・12 刑集 57 巻 3 号 322 頁）、不当利得返還請求の対象になる場合もある。

このようなファイナリティに関する精緻な議論が発展したのは、資金決済が多数の銀行がメンバーとなっている銀行間決済システムを介して行われ、ファイナリティが否定されると、ある銀行の破綻が決済システムを介して他の銀行に波及し、金融システム、ひいては経済全体の危機を招きかねないという、システミック・リスクの問題が生じるためであった。しかし仮想通貨の場合は、多数の銀行をメンバーとする決済システムを構成しているわけではなく、決済において銀行間の与信関係が生じるわけではない。仮想通貨そのものに価値があるとされ、仮想通貨の移転によって決済がなされるのである。従って、システミック・リスクが生じることは考えにくい。ファイナリティが問題になるとすれば、どの時点において仮想通貨の移転が完了し、その効果が覆されなくなるか、そしてそれによって仮想通貨を授受した当事者間において債務の弁済の効力が生じるかという、当事者間完了性の問題であろう。そこで本報告においては、債務の弁済のために債務者が仮想通貨を送付した場合に債権者に対する弁済の効力が確定的に発生する時点、即ち、当事者間完了性を中心に検討したい。

尤も、わが国において仮想通貨を保有している人の殆どは、自らの独立した仮想通貨アカウント（ノード）を保有して、秘密鍵を持っているわけでなく、ネットワーク参加者である仮想通貨交換業者から仮想通貨を購入して、当該業者に仮想通貨を預けているだけのネットワーク非参加利用者に止まっているようである。現在、ビットコインによる支払を認めているとされるビックカメラは、仮想通貨そのものの移転によって支払を受けているわけで

はなく、顧客が仮想通貨を預けている仮想通貨交換所（ビットフライアー）が、支払金額に相当する顧客の預託分の仮想通貨を取り崩して、現金でビックカメラに対価を支払っているようである。これは結局、現金による決済の一形態であり、むしろ資金決済法の問題となることから、本報告では扱わないこととする。

（２）当事者間完了性

当事者間完了性とは、当事者間で決済が最終的に完了することを指すとされる。債務者が、仮想通貨を決済手段として債権者に送ったことによって、当該債権者に対する債務を弁済したことになり、債権が消滅するのが、当事者間完了性である（民法 473 条・482 条。UNCITRSAL Model Law on International Credit Transfers (1992), Article 19 参照）。

（３）対第三完了性

これに対し、対第三者完了性とは、受取人（債権者）側からみて、いったん資金を受け取れば、事後的に第三者から所有権やそれ以前の原因関係に基づいて返還を請求される恐れがないということを指す。債務の弁済として仮想通貨を受け取った債権者が、第三者から当該仮想通貨は第三者のものであるなどとして、当該仮想通貨の返還を求められることがないことが、対第三者完了性である。対第三者完了性としてのファイナリティからは、第三者との関係でも決済が有効とされ、決済に係る行為が倒産法等との関係でも遡及的に影響を受けないことになる（Benjamin Geva, Settlement Finality and Associated Risks in Funds Transfers-——When Does Interbank Payment Occur?, 22 Penn State International Law Review 33 (2003)）。具体的には、銀行間の振替指図のネッティングの効力が、倒産手続きが宣告されると、その効果が倒産手続開始日の真夜中 0 時にまで遡及するという、オーストリア、ギリシャ、イタリア、オランダ等におけるゼロ・アワー・ルールによって覆されないこと等を、EU のファイナリティ指令は規定している（（Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities systems, OJ L166, of 11 June 1998, at 45~50 Article 3 et seq.）。

（４）資金決済完了性

資金決済完了性とは、追加的な資金決済が必要ではなく、支払自体として完結していることを指す。手形交換を介する小切手による支払の場合、小切手を受け取った債権者が、当該小切手を自己の取引銀行の自分の口座に入金しても、手形交換で当該小切手を持ち帰った支払銀行が不渡返還を行わないことが確定する手形交換の翌日になって、初めて資金決済完了性が得られることになる。これに対し日銀ネットにおいては、RTGS モード、LSF モードを用いた決済を行うことにより、支払指図が受信銀行に受信されると直ちに送受信銀行間の決済を行って、資金決済完了性を速やかに実現させている。全銀システムも、１件１

億円以上の大口内為取引については、日銀ネットに送付され、LSF 口座において日銀ネットによる LSF モード決済が行われる。日本銀行からの決済終了通知を受け取った全銀システムは、保留していた支払指図を受取銀行に送信し、受取銀行は受取人の口座に入金記帳を行う。このように速やかな資金決済完了性を実現している。尤も、1 件 1 億円未満の小口内為取引については、1 日 1 回、全銀センターが参加銀行ごとの受払（送信金額と受信金額）の差額を算出して日本銀行にオンラインで通知し、日本銀行は決済時刻（通常は 16 時 15 分）に各銀行が日本銀行に有している当座預金口座につき当該差額を引落または入金をして、決済を完了させる。

このように資金決済完了性は、送受信銀行の日銀当座預金口座による決済時点で実現されるが、内国為替取扱規則とそれを受けた各銀行の預金規定の定めにより、資金決済完了時点を待たずに、送信銀行（仕向銀行）から全銀システムにより送信された支払指図を受信銀行（被仕向銀行）が受信した時点で、受信銀行が振込の受取人の口座に入金記帳し、資金解放することにしている。当事者完了時点を資金決済完了時点より早めているわけであり、送信銀行の決済不能リスクは全銀システムの CCP（Central Counter Party：中央清算機関）である全銀ネットがいったん負担する。しかし、仕向超過限度管理制度によって決済不能リスク額は抑制され、参加銀行から全銀ネットへの担保・保証の差入、ロスシェア・ルールによって、決済不能金額は決済参加銀行（デフォルターズ・ペイ、破綻行支払）が最終的に負担することになっている（中島真志＝宿輪純一『決済システムのすべて[第 3 版]』（東洋経済新報社、2013 年）311 頁以下）。以上のように当事者完了時点を資金決済完了時点より早めているのは、受取人が振込金を早く受け取れるようにして、全銀システムによる送金サービスの質を高めるためと考えられる。

（５）撤回不能性

支払指図の撤回不能性は、支払指図を発した者は、どの時点まで当該支払指図を撤回できるかという問題である。振込を例にすれば、大阪地判昭和 55・9・30 判時 998 号 87 頁は、先日付の振込依頼につき、振込の意思表示が発効する振込指定日より前に振込の意思表示を撤回する組戻の意思表示が被仕向銀行に到達していれば、振込の意思表示は効力を生ぜず、受取人の預金債権は成立しないとした。東京高判昭和 62・10・28 判時 1260 号 15 頁は、仲介銀行を経由して被仕向銀行（農協）に振込依頼した振込依頼人が、振込委託を撤回して仕向銀行に対し振込金の返還を請求したが、仕向銀行が振込指図を仲介銀行に送信し、振込金を送金した時点において、振込委託は撤回不能になると解して、請求を棄却した。東京地判平成 5・3・5 判時 1508 号 132 頁は、先日付振込委託を受けた仕向銀行が、振込日前に振込を実行してしまったために、仕向銀行が受取人を被告に振込金の不当利得返還請求を求めた事件であるが、「振込依頼の撤回は、振込委託契約の解除と解されるから、一般に被仕向銀行における受取人口座への入金記帳前には自由にできる」として、仕向銀行の請求

を認めた。このように支払指図の撤回不能時点については、受取人口座への入金記帳時とする考えと、送信銀行による支払指図の発信及び送金を実行した時点とする考えがあった（岩原・前掲 260 頁以下）。

この他、アメリカの U.C.C. Article 4A-に関しては、支払完了性（payment finality）または受領者完了性（receiver finality）と債務完了性（obligation finality）が分けて論じられている。支払完了性または受領者完了性とは、被仕向銀行が受取人に支払（資金解放）を行った以上は、受取人に対する支払を取り消したり、撤回することが認められないというものである。これは、仕向銀行との間で被仕向銀行が支払指図の資金決済を完了していない時点で受信銀行が受取人である顧客に資金解放をした場合、たとえその後、受信銀行が送信銀行から決済資金を受け取ることができなくても、受取人への支払を取り消したり、撤回できないということである。送信銀行と受信銀行の間の資金決済が行われるという条件付きの資金解放を認めないということで、アメリカの振込に関する UCC § 4A―405(c) は、こういう意味での支払完了性を原則として規定している（ACH と CHIPS 等に関する例外が認められている。UCC § 4A―405(d)(e)）。わが国においては、普通預金規定等の約款上は、入金記帳の取消事由として銀行間の決済不能を挙げていない。

債務完了性は、EU のファイナリティ指令で用いられている概念である（Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities systems, OJ LI 166, of June 1998, at 45～50, at Preamble (13)）。即ち、システミック・リスクを発生させないために、決済システムにおけるネッティングの効力が否定されず、入力された振替指図（transfer order）が撤回されず、正常に決済されることをいうとされる（嶋・前掲 4 頁～5 頁）。詐欺（fraud）や、エラーなど支払の原因債権から生じる権利や不当利得返還請求権の行使は妨げられない。

２　ブロックチェーンにおける送金の仕組み

（１）序

仮想通貨のファイナリティを問題にするとき、ビットコインのようなブロックチェーン技術を用いた仮想通貨による支払のファイナリティが特に問題とされていると思われることから、ブロックチェーンにおけるファイナリティの問題を検討したい（以下は、小出篤「「分散型台帳」の法的問題・序論」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』（有斐閣、2017 年）827 頁に多くを負っている）。

ブロックチェーンにも、特定の管理者のいないパブリック型と、管理者が複数いるコンソーシアム型と、管理者が単数のプライベート型に分かれるとされる（「ブロックチェーン技術の活用可能性と課題に関する検討会報告書――ブロックチェーン技術が銀行業務に変革をもたらす可能性を見据えて――」（2017 年 3 月 16 日）13 頁（以下、「検討会報告書」と略す）、片岡義広「ブロックチェーン技術と金融機関関連の法制度的論点についての報告書」

（2017 年 7 月 3 日）2 頁、「「証券取引における分散台帳技術の利用を巡る法律問題研究会」報告書――証券決済制度と分散台帳技術――」日本銀行金融研究所（2017 年 11 月）4 頁以下。http://www.boj.or.jp/announcements/release_2017/rel171109a.htm/（以下、「金研報告書」と略す））。パブリック型の代表がビットコインであり、コンソーシアム型の代表がリップルである（Microsoft、MIT、CGI 等 55 の管理者（validator）の合意により承認が行われる）。

（２）ブロックチェーンの仕組みと送金

ブロックチェーンとは、支払等の仮想通貨の取引データをすべて記録する台帳データである。あらゆる仮想通貨取引データを、一定期間ごとに一つのブロックに格納してつなげている。この台帳データは、パブリック型の場合、特定の者によって管理されているわけではなく、ネットワーク全体で管理され、公開されている。ネットワークに参加する端末（ノード）すべてにおいて台帳データは常に同期され、原則として同一の内容のものとされている。ネットワーク参加者は、非対称鍵暗号方式により固有の公開鍵と秘密鍵のデータを有する。

以下、ビットコインを例にブロックチェーン技術を用いた仮想通貨による送金手続きを説明する。ビットコインにより送金したい者は、受取人を特定するためのデータとして、受取人の公開鍵のダイジェストからなる識別子や、送金する資金に関するデータとして、送金者に入金された過去の取引のデータのダイジェストなどに、送金者のデジタル署名を施したうえで、送金のデータをネットワーク上に発信する。このような送金データは、「マイナー（miner: 採掘者）」と呼ばれるネットワーク参加者によって収集され、一定期間ごとに一つのブロックにまとめて格納される。このブロックには、その期間中のすべての送金取引のデータに、生成取引と呼ばれるデータが付け加えられて格納される。生成取引は、このブロックのマイナーに対して一定量のビットコインを送金する取引である。世界中のマイナーは、このブロックについて「マイニング（mining: 採掘）」と呼ばれる行為を競走して行う。当該ブロックについて世界で最も早くマイニングに成功した 1 人のマイナーのみが、そのブロックを既存のブロックチェーンの末尾に付記することができる。そしてこれをネットワーク上に送信する。それにより、新たなブロックが追加された新しいブロックチェーンが当該仮想通貨のネットワークに参加するすべての「端末（ノード）」に同期され、マイニングに成功したことが検証されたうえで承認される。マイニングの成功により、当該ブロック内の送金取引が承認されるとともに、生成取引も承認される。生成取引はシステム上、新たに仮想通貨が発行されたものと扱われ、マイニングの報酬とされる。マイナーはこの報酬としての仮想通貨をシステムから得るためにマイニングを行う。ブロックチェーンの仕組みを運用するための費用は、このようにしてなされるマイナーへの仮想通貨の追加発行という報酬により担われているわけである。仮想通貨の追加発行は、仮想通貨の価値をその分だけ水割りすると考えられるため、ブロックチェーンの維持・運営費用は当該仮想通貨を所有

する者全員によって負担されていると言えよう。

このマイニングとは、ある条件を充たす「ノンス」と呼ばれるデータ（32 ビット長のデータとされる）をいち早く見つける競走である。その条件とは、①当該ブロック内のすべての取引データをハッシュ化したダイジェストと（「マークル・ルート値」と呼ばれる）、②直近の承認済のブロック（現在のブロックチェーンの末尾のブロック）のマイニングの際に得られたダイジェストと、③任意のノンス、以上 3 つの要素からなるデータをハッシュ化して得られるダイジェストが、一定数以上連続した「0」から始まるものであること、である。①、②は既定の数字であることから、マイナーは③のノンスを変化させながらハッシュ化の計算を行い、得られるダイジェストが条件を充たすノンスを探す。

ハッシュ関数においては、特定のダイジェストをもたらす元データを計算によって導くことは不可能なことから、総当り的にいろいろなノンスを試してみるしかなく、他のマイナーより早くマイニングに成功する確率は、マイニングに使用しているコンピュータの性能に依存する。1 つのブロックごとにマイニングが約 10 分に 1 回の割合で成功するように、条件は設定されている。コンピュータの計算速度の総量が上がれば、条件を更に厳しくして（例えば、必要な連続する「0」の数を増やす）、常に 10 分に 1 回の割合でマイニングが成功するように自動的に調整されている。なお、マイニングに成功したことを他の者が検証することは、ハッシュ関数に答えとされたノンスを含むデータを代入して得られるダイジェストが条件に合致しているかを確認すればよく、1 回の計算でできるため、極めて容易である。

このようにマイニングという困難な作業に成功したこと（コンピュータの能力を投入したこと）によりブロックチェーンのブロックの正当性を保証する考え方を、”Proof-of-Work”と呼ぶ。パブリック型のブロックチェーンは、中央管理者が存在しないため、複数のマイナーがほぼ同時にマイニングに成功して別々のブロックをネットワーク上に送信した場合、ネットワーク障害により取引データやブロックが一部のノードに送信されなかった場合、参加ノード間でタイムラグが生じる場合等に、ブロックチェーンの分岐が発生し得るとされる。あるブロック以後に複数のブロックチェーンが分岐して発生した場合、より長いチェーンが形成された方が正当なブロックチェーンとして採用される。長いチェーンにはよりコストが投入されていると考えるためである。この判定は、参加ノード内の多数派が認めたブロックを正とすることにより行われる（ここからいわゆる 51%問題が生じる）。そのため、あるブロックについてマイニングが成功してブロックチェーンが追加された後も、それが短い間は、そのときに分岐が生じていた場合は、他のブロックチェーンに長さを超されて、当該ブロックが廃棄されてしまうことがあり得る。そこで、当該ブロック以後に 5 個のブロックがチェーンされて初めて、当該ブロックの取引はほぼ覆ることはないと考えられている。その結果、約 10 分に 1 回のペースでマイニングが成功するようにノンスの条件は調整されていることから、取引の承認がほぼ安定するまでに 6 個のマイニングに要する約 60

分がかかることになる。しかもビットコインでは、手数料が高い取引が優先的に承認され、低い取引が承認されない等の事象が存在するといわれ、72 時間経過すると記録が消滅してしまうといった問題も指摘されている（検討会報告書 21 頁）。

（３）ブロックチェーンと改竄、巻戻し

以上のようなブロックチェーンの仕組みからくる特徴として、いったんブロックチェーに追加されたブロックについて、事後的に改竄することが極めて困難であるとされる。ハッシュ関数の特性として、ある取引データを改竄すると、当該ブロックの中のマークル・ルート値が今までと全く違ったものとなり、ネットワーク上の検証プロセスではねられてしまうことになる。それを避けるためには、改竄者は当該ブロックにつきマイニングを自分だけで成功させなければならない。当該ブロックにつき再度のマイニングに成功しても、その結果得られるダイジェストもこれまでと全く異なるものになるため、連結された次のブロックのマイニングの対象データに含まれることから、次のブロックについても、改竄者は自分だけでマイニングを成功させなければならない。結局、取引データを改竄したブロック以降のすべてのブロックにおける取引データにつきマイニングをやりなおさなければならない。しかもその間にも、他の当該仮想通貨取引は世界中で進行し、10 分に 1 回の割合で新しいブロックが追加されることから、改竄者は、他のマイナーの単位時間当たりの総計算量を超えるスピードで計算して、改竄したブロック以降のデータをすべてマイニングし直さなければ、現在のブロックチェーンの長さを超える新しいブロックチェーンを作出することはできない。すべてのマイナーの総 CPU 処理能力の 51%以上を保有しなければそれはできないことから、ほぼ不可能と考えられている。しかしこのことは逆に言えば、総 CPU 処理能力の 51%以上を保有する者が現れた場合は、Proof-of-Work による信頼は確保できないことを意味する（51%問題）。

以上のようにブロックチェーンにおいては、ブロックの取引データは、承認されると改竄することができないし、必要な訂正を行うこともできない。訂正の代わりに、当事者間で巻戻し取引（反対取引）を行って、ブロックチェーンに新たなブロックを追加するという方法を取らざるを得ない。そこで通常は、ビットコインによる支払は、マイニングに成功して承認され、ブロックが追加された約 10 分後の時点で支払があったものとするのが通常ではないかと思われる。より慎重に 6 ブロックの追加がある約 60 分後に支払が確定すると考える慣行もある。しかし前述したように。約 60 分経過しても覆される危険はなくならないわけである。

３　ブロックチェーンとファイナリティ

（１）ビットコインによる支払のファイナリティ

仮想通貨による支払のファイナリティという問題を考えるためには、仮想通貨の法的性

質とか、仮想通貨取引に適用される法は何かといった問題をまず検討する必要があるはずである。しかしこれらの問題に関し未だ確定的な見解は確立されていない。そこで以下においては、ビットコインやRippleといった代表的な仮想通貨の仕組みや運用から分かる範囲で、これらによる支払のファイナリティの問題を考えてみたい。

２に記したようなビットコインの特色からは、ファイナリティの問題はいかに考えられるか。まずビットコインで送金を行っても、ブロックの追加は10分に1回程度とされていることから、その取引が承認されるのに10分程度はかかる。しかもノード間の距離が離れていると合意形成に要する時間は長くなると言われており、また、ノードの数を増やすと、合意形成に要する時間はどんどん増加していくとも言われる。ビットコインの場合は、２で述べたように、コンセンサスアルゴリズムにおいてProof-of-Workの仕組みを採っていることから、チェーンに分岐が生じて、たとえ承認を得た取引であっても、 より長いチェーンが出てくると、結果が覆されるという問題もある。そのため慣行として、60分程度待って（6ブロックが進んで）から次の取引を依頼するということが行われている。しかし60分まったからといって、覆される可能性が全くなくなるわけではないことから（遅いときは支払の完了に数日かかることもあると言われる）、ネットワークとしてファイナリティに欠けると評されている（検討会報告書12頁）。

法的に見た場合、仮想通貨による支払は、送信される仮想通貨自体が価値を持つ決済手段であるため、支払指図の送信とは別に仕向銀行と被仕向銀行間の資金決済が必要な振込のような問題はないため、資金決済完了性の問題は生じない。しかしProof-of-Workの仕組みを採っているビットコインによる支払は、承認手続きにも10分程度かかって、即時性がないだけでなく、２（２）で論じたように、たとえ当該ブロックが承認を得ても、ブロックチェーンに分岐が生じて、別のより長いブロックチェーンが多数派に承認され、当該ブロックは無効とされる可能性がある。そうすると、たとえビットコインによる支払が承認を受けても、支払の効力が覆される可能性があるため、支払完了性または受領者完了性、債務完了性（以下、「支払完了性等」と呼ぶ）が認められないことになる。従って、ビットコインの送付につき承認を受けた時点においても、債権者が確実な弁済を受けたとは言えず、当事者間完了性は認められないのではなかろうか。そうなると、対第三者完了性を認めることも難しいのではなかろうか。一般にProof-of-Workの仕組みをとっている場合、ファイナリティを確定できないとされている（ブロックチェーンに関する法と技術研究会「ブロックチェーンの可能性と課題――法と技術の対話――」金法2076号（2017年）6頁・12頁）。

仮に送金の指図がネットワークによって参加者に届いて承認を受け、ブロックの追加が行われても、更に言えば慣行に従いブロックの追加から60分待って次の取引の依頼が行われたとしても、当該ブロックチェーンよりより長いブロックチェーンが分岐によって形成されていたことが分かれば、長いブロックチェーンの方が有効とされ、短い当該ブロックチェーンの支払の効力は否定されることになる。承認を受けた時点で当事者間完了性や対第

三者完了性が実現すると言えるのか、慣行に従い 60 分まてば実現するのかと問われれば、支払完了性等がない以上、いずれの場合も法的には当事者間完了性も対第三者完了性も認めることもできないと言わざるを得ないであろう。

このような状況は、小切手による支払を受けた受取人が、取引銀行である取立銀行の自分の口座に小切手を入金した場合に似ていると言えよう。取り敢えず小切手金額が仮入金記帳されるが、当該小切手が手形交換に付されて、支払銀行からの不渡返還なしに不渡返還期限が経過する交換日の翌営業日の午前 11 時までは、取立銀行は原則として小切手金の資金解放には応じず、仮入金記帳に当事者間完了性や対第三者完了性を認めることはできないと考えられている。この考え方からは、ビットコインにおいてはブロックチェーンの分岐の結果、ブロックの追加の効力、従ってビットコイン送金の効力の承認が取り消される可能性がいつまでも存在する以上、厳密に言えば、支払のファイナリティはいかなる意味においても（支払完了性等も、当事者間完了性も、対第三者完了性も）いつまでも認められないことになりそうである。

このようなことから、ビットコインのようなパブリック型のブロックチェーン技術を用いた仮想通貨は、少なくとも支払の即時性が求められる店頭等における消費者取引等の支払手段には、向かないように思われる。リテールの送金取引一般についても、全銀システムが資金決済完了時点よりも当事者間完了性、対第三者完了性、支払指図の撤回不能性等を早めて、支払の即時性を実現しているのと比較すると、ビットコインはファイナリティの点で支払手段として劣っていると言えよう。尤も、支払の即時性が求められず、支払の確実性が厳密に求められず、安価性が重視される送金（ロー・バリュー送金)、例えば海外への大量送金等については、ビットコインが用いられる可能性があるのかもしれない（検討会報告書 27 頁)。あとはビットコインが非常に普及した場合に、送金の承認後にその効力が覆される危険を承知で、そのようなことは稀であろうとして、債権者がビットコインによる支払を受け入れる可能性があり得るのかもしれない。アメリカにおける小切手による支払の普及がそのような例である。

（２）コンソーシアム型またはプライベート型ブロックチェーンにおけるファイナリティ

コンソーシアム型またはプライベート型ブロックチェーン技術を用いた仮想通貨においては、ファイナリティを早期に実現することも可能かもしれない。それを可能とするアルゴリズムとして、例えば、Practical Byzantine Fault Tolerance （PBFT）がある。これはネットワーク参加者の一人がプライマリ（リーダー）となり、自らを含む全参加者（ノード）に要求を送り、その要求に対する結果を集計して多数を占めている値を採用することでブロックを確定させる仕組みである。この場合、ブロックを確定した時点で仮想通貨は確定的に受取人のものとなり、仮想通貨による送金は取消不能となって、仮想通貨による弁済の合意が認められれば、送金人から受取人への支払による弁済の効力が発生し（民法 473 条・

482 条。当事者間完了性)、それは送金人の破産管財人等の第三者も争うことができないと考えられる（対第三者完了性)。尤も、詐害行為取消、不法行為、不当利得等の一般民事上の救済があり得ることは別である。

PBFT のような仕組みは、参加者が増加すると合意形成に要するメッセージ量が指数関数的に増え、合意形成にかかる時間も長期化するため、通常は全体のノード数に上限を設けている（一般的にはノードの数は 10 から 20 くらいの参加者が適当とされる)。それを超えると実用性に影響するとの指摘もある。代表的なコンソーシアム型のブロックチェーン技術を用いた仮想通貨である Ripple は、数秒で支払を実現することができると言われる。ところが Ripple には Validator が 55 名もいる。その間でなぜ数秒で承認の意思決定ができるのか不明である（検討会報告書 13 頁、ブロックチェーンに関する法と技術研究会・前掲 13 頁参照)。しかしそのようなことが可能であるならば、ファイナリティの問題を解決でき、送金の確実性とスピードを兼ね備えた送金システムとなり得よう。この意味で、仮想通貨を用いた送金サービスを検討しているわが国の銀行が、Ripple を使用することを計画していることは興味深い。例えば、2016 年 10 月 25 日に、SBI グループ等の 42 金融機関は、「国内外為替の一元化検討の一元化検討に関するコンソーシアム」を立ち上げて、Ripple の決済基盤を用いたプラットフォームを構築し、ブロックチェーンを活用した決済サービスの実用化を目指している（「次世代決済サービス」金財 2016 年 11 月 21 日号 10 頁以下)。また、証券振替決済制度に分散台帳技術を応用する場合も、PBFT を採用することが提案されている（金研報告書 37 頁)。

なお、ブロックチェーン技術を用いた仮想通貨による決済については、全銀システムや日銀ネットのような中央集権的な大規模システムと異なり、コストが低いと思われており、それが大きな魅力と感じられているようであるが、ビットコインなど、マイニングをするためのコンピュータを稼働させる電気料金等が高額にのぼっており、マイナーにその対価として新たなビットコインを提供しているために表面化していないが、実は、ビットコインには普通の銀行システムを作るより高いコストがかかっているという指摘があることに留意すべきであろう（赤羽喜治＝愛敬真生編著『ブロックチェーン　仕組みと理論――サンプルで学ぶ FinTech のコア技術――』（リックテレコム、2016 年）15 頁以下)。しかもマイニングのコストはビットコインの入手のためだけにかけられる費用で、社会的に無駄なコストではなかろうか（Ripple は、マイニングではなく癌などの研究開発に貢献すると Ripplecoin がもらえる。日本銀行券の発行益は日銀納付金として国庫に繰り入れられる)。

（３）BIS「金融市場インフラのための原則」原則 8 と仮想通貨のファイナリティ

BIS「金融市場インフラのための原則」原則 8（以下、「BIS 原則 8」と略す）は、「FMI（金融市場インフラ）は、最低限、決済日中に、ファイナルな決済を明確かつ確実に提供すべきである。」、「FMI は、必要または望ましい場合には、ファイナルな決済を日中随時にま

たは即時に提供すべきである。」としている。そしてその「重要な考慮事項」においては、「FMI の規則・手続きは、決済がいつの時点でファイナルとなるのかを明確に定義すべきである。」、「FMI は、決済リスクを軽減するため、決済日中に、（より望ましくは）日中随時または即時に、ファイナルな決済を完了すべきである。……」、「FMI は、決済未了の支払・振替指図・その他の債務を参加者がいつの時点以降に取り消すことができなくなるのかについて明確に定義すべきである。」としている。

仮想通貨による支払は、前述したように、仮想通貨の法的性質も仮想通貨支払に適用される法も不明な現状では、BIS 原則 8 を充たすものか、不明と言わざるを得ない。しかし上述のようなファイナリティに関する検討からは、ビットコイン等のパブリック型のブロックチェーン技術を用いた仮想通貨は、支払完了性等を充たせないことから、BIS 原則 8 の要件を充たすことが困難と考えられる。これに対し、コンソーシアム型またはプライベート型のブロックチェーン技術を用いた仮想通貨は、支払完了性等を充たし、支払が取り消されなくなる時点を明確にすることも可能で、支払の即時性もほぼ充たす可能性があることから、BIS 原則 8 の要件を充たす可能性があるのではないかと考えられる。尤も、そのことを明確にするためには当該仮想通貨に係る法制や約款を整備する必要があろう。