第６章　キャッシュレス決済手段としての仮想通貨
ー分散型仮想通貨による決済手段性とファイナリティの実現性ー

岡　田　仁　志

I. 仮想通貨の決済手段性

仮想通貨の代表例としてのビットコインは、2008年にサトシナカモト名義の人物が暗号学のメーリングリストに投稿した論文を元に実装されたビットコイン・システムによって表現された金銭的価値である。仮想通貨に決済手段性を認めることの当否については諸説あるが、複数の国家においては法体系において決済手段性が認められている。

わが国においては、改正資金決済法が2017年4月に施行されたことを受けて、仮想通貨の法的性質が定義された。改正資金決済法2条5項1号および同2号の文言は、仮想通貨が決済手段性を備えていることを前提としているものと読み取ることができる。

1. 資金決済法による決済手段性の定義

(1) 資金決済法２条５項１号

資金決済法2条5項1号によれば、仮想通貨とは「物品購入・サービス提供を受ける場合に、代価の弁済のために不特定の者に対して使用できるもので、かつ、不特定の者を相手方として購入及び売却ができる財産的価値で、電子情報処理組織を用いて移転できるもの」と定義される。

最初の「物品購入・サービス提供を受ける場合に、代価の弁済のために」利用されるというのは、仮想通貨が決済手段であるということを意味する。仮想通貨がモノであるならば、物品を購入する際には、商品としてのモノと仮想通貨というモノを物々交換することになる。現金に代えてモノで支払うという代物弁済と見ることもできよう。しかしながら、改正資金決済法によって、仮想通貨は決済手段としての地位を与えられたといえる。

次に、「不特定の者に対して使用できるもので」という要素は、汎用性に該当する。これは国内のあらゆる業種で利用できることを意味する。汎用性という要素は、電子マネーにも備わる性質である。汎用性を有しないとされるゲーム内通貨などの内生的な手段とは異なり、仮想通貨には汎用性が付与されたと解することができる。

第三の要素は、「不特定の者を相手方として購入及び売却ができる」という文言である。これは、転々流通性のことを指すといえる。仮想通貨というのは、誰から誰にでも移転で

きる金銭的価値である。電子マネーが制度的に個人間の移転を制限するのとは対照的に、仮想通貨は無制限の転々流通性にこそ機能的意義が求められると考えられる。

(2) 資金決済法２条５項２号

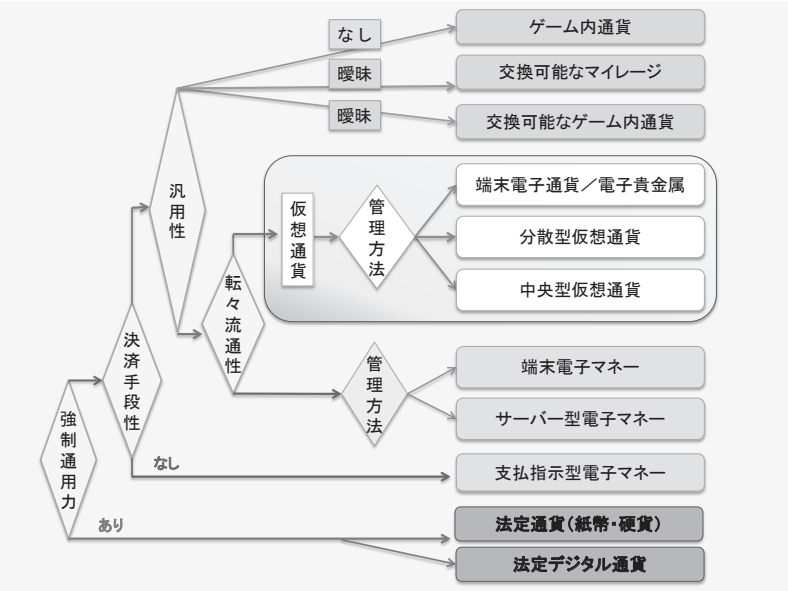
資金決済法2条5項2号では、1号で定義した仮想通貨と交換可能なものを2号仮想通貨と定義する。すなわち、「不特定の者を相手方として(前号で定義したものと)相互に交換を行うことができる財産的価値で、電子情報処理組織を用いて移転できるもの」は、仮想通貨に該当すると定義する。同号は、仮想通貨の範囲を補完的に定義する条項であると解される。

2. 仮想通貨の定義の外延

資金決済法が定義する仮想通貨というのは、ビットコインに代表される分散型仮想通貨を指すのか、発行者が存在する中央型仮想通貨を指すのかは、文言上は特定されていない。すなわち、資金決済法が定義する仮想通貨とは、仮想通貨取引所が取り扱う客体としての仮想通貨の外延を決定するためのものであって、仮想通貨そのものの性質を定義したわけではない。

改正資金決済法2条5項1号および同2号が定義する仮想通貨の性質は、既存の電子マネーなどの性質との比較において分類するならば、図表1のように鳥瞰することができる。

図表1　仮想通貨の特性と決済手段における位置付け



（出所）岡田仁志・高橋郁夫・山崎重一郎 (2015)から作成。

II. 仮想通貨のファイナリティ

仮想通貨がキャッシュレス手段として利用されるためには、債務を消滅させることのできる弁済の効果が認められなければならない。そのためには、仮想通貨の移転を以て、第三者からの抗弁を受けることなく、終局的に弁済としての効果が得られなければならない。

仮想通貨に弁済の効果が認められるか否かは、中央型仮想通貨においては専ら発行企業と利用者との間で締結される約款の文言に依存する。これに対して、分散型仮想通貨の例においては、発行企業が存在しないため、プログラムの命令すなわちCODEによって表現された性質に依拠する。

1. 仮想通貨の貨幣的性質

理想的電子現金の条件について論じた岡本龍明・太田和夫(1991)は、電子現金が備えるべき6項目を提案した(図表2)。この条件に照らしてみると、ビットコインは独立性、安全性、転々流通性、分割可能性については条件を充たしている。プライバシーについては所有者を識別するためのビットコインアドレス同士の取引の関連性を捕捉可能なため完全とはいえないが、アドレスと所有者の実名の紐付けは一般にはできないため、一般的な意味でのプライバシーは確保されているといえる。オフライン性については満たしていないが、現在のネットワーク環境に鑑みれば大きな問題にはならないと考えられる。

図表2　理想的電子現金の6条件

	理想的電子現金の条件
独立性	物理的な耐改ざん性や信頼できる第三者機関に依存しない
安全性	コピーして二重払いに使用できない
プライバシー	流通する使用者の追跡や取引内容などの保護
オフライン性	支払い時にプロトコルがオフラインで実行できる
転々流通性	使用者間を転々と流通可能である
分割可能性	少額に分割して支払いに充てることが可能である

（出所）岡本龍明・太田和夫（1991）

2. 分散型仮想通貨のファイナリティ

分散型仮想通貨においては、ブロックチェーン技術を利用することによって、トランザクションの存在を不可逆的に固着化すること、および、トランザクションの存在を公知するこ

とを可能にしている。これによって、トランザクションを改竄することも、トランザクションの存在を否認することもできない効果が得られる。

発行主体の存在しないピアー・ツー・ピアー(P2P)のネットワークにおいては、参加者の一部が結託することによって事実とは異なる記録を創出することができる。これはビザンティン将軍問題と呼ばれる難問であるが、ビットコイン・システムは、競争的にブロックを生成するマイニングのプロセスによって、結託の可能性を十分に極小化することを可能にした(図表3)。

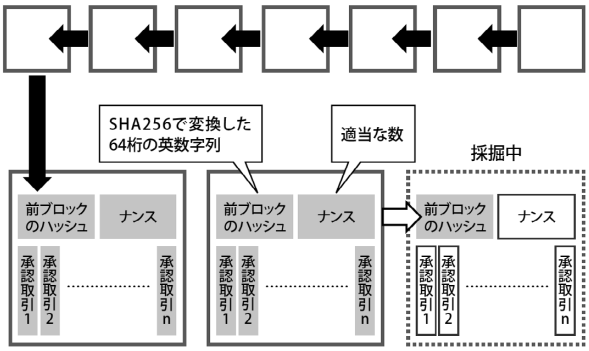
しかしながら、分散型仮想通貨が表現するファイナリティは理論的に証明されたものではなく、むしろビザンティン将軍問題には解決法がないとする証明の正しさが維持されているものと考えられている。すなわち、ブロックチェーンによって実現される終局的な記録の効力というものは、社会的にみて十分に誤りの可能性が低いとして受容することによってのみ正当化されるものであり、誤りの可能性を完全に排除するものではない。

分散型仮想通貨として最も長い歴史を持つビットコイン・システムにおいては、自由参加型のノードが地理的かつ論理的にみて十分に分散していること、ブロックを生成するマイニングの作業に投入されるハッシュパワーの量が十分に大きいこと、および、継続的な攻撃に対する改ざん耐性を持つことなどを総合的に判断して、社会的にみて相当な程度のファイナリティが実現されているとする見方もある。

これに対しては、ブロックチェーンの耐改ざん特性を測定する手法が確立されていないこと、自由参加型のノードが地理的かつ論理的に集中して結託する可能性を排除できないこと、投入されるハッシュパワーの供給が途絶するリスクを否定できないことなどを根拠として、決済手段に求められる程度のファイナリティを実現していないとする見解もあり得る。

思うに、分散型仮想通貨は発行主体が存在しないにもかかわらず相当な程度のファイナリティを表現していることに意義が求められるのであるから、契約の両当事者がそのファイナリティの程度を受容する限りにおいて弁済の効力が認められると解するべきであり、すなわち強制通用力を備えない任意通貨としての性質に止まると理解するのが妥当であると考える。

図表3　分散型仮想通貨のマイニング過程



（出所）岡田仁志（2018）

3. 中央型仮想通貨のファイナリティ

分散型仮想通貨とは対照的に、中央型仮想通貨においては明確な発行者が存在している。この場合にあっては、特定信頼点としての発行企業がデータベースの真正性を担保するのであるから、必ずしもブロックチェーン技術を活用する必然性は認められない。もっとも、不可逆的な記録を残すための方法として、従来のデータベースによる構成に代わるものとして、ブロックチェーンもしくは分散台帳技術を応用して導入することも可能である。

ブロックチェーンおよび分散台帳技術の定義と分類に関しては、国際標準化団体における議論が進められるものと考えられているが、現状においては広く受容される定義もしくは分類論というのは存在していない。分散型仮想通貨であるビットコインとの対比において、中央型仮想通貨の性質を定義するならば、図表4のように理解することができる。

ビットコイン・システムのような分散型仮想通貨に使われるブロックチェーンは、ノードとしてネットワークに参加することに許可を必要としない。ブロックを生成するマイナーが参加するインセンティブは、マイニングの報酬として得られるコインベースであって、これには市場が形成される。このようなブロックチェーンは、市場型であり、自由参加型である。

中央型仮想通貨を構成する場合には、ノードとして参加する主体を許可するための特定信頼点が存在する。この分類はさらに、コインベースを付与して一般ノードの参加を得る許可型パブリックチェーンと、許可ノードだけで構成するためインセンティブとしてのコインベースを必要としない許可型コンソーシアムチェーンとに区分される。前者は、一般ノードと許可ノードが混在するため、市場型かつ許可型である。後者は、許可ノードのみで構成されるため、非市場型であって、許可型である。

前者のファイナリティは、ブロックチェーンに投入されるハッシュパワーの程度および許可主体の信頼性に依存する。後者のファイナリティは、専ら許可主体である幹事企業の信頼

性に依拠し、許可ノードを構成する企業の信頼性がこれを補完する。なお、ノードが1個であって市場性を持たないプライベートチェーンは、ブロックチェーンもしくは分散台帳技術の定義には含まれず、従来型のデータベースの改良と位置付けることができよう。

図表4　ブロックチェーンの分類（市場と許可の観点から）

	単独型	許可型	自由参加型
市場型		許可型パブリックチェーン	パブリックチェーン
非市場型	プライベートチェーン	許可型コンソーシアムチェーン	

（出所）岡田仁志 (2016b)から作成。

III. 仮想通貨の価値の所在

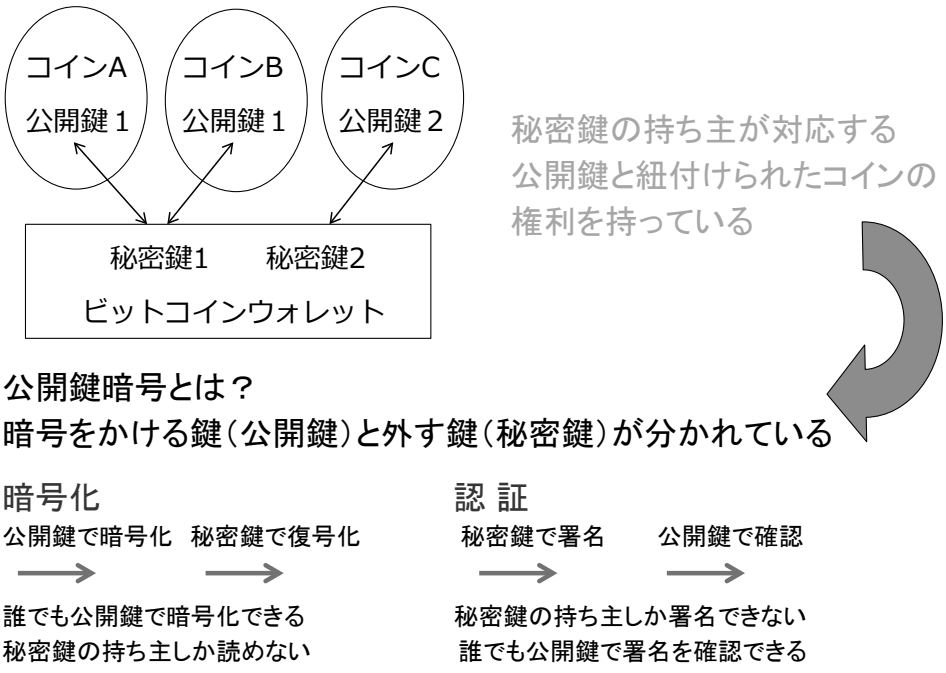
仮想通貨をキャッシュレス手段として活用するためには、これを利用する消費者が安全に価値を保有することができなければならない。すなわち、個人の仮想通貨アドレスに紐付けられた価値を排他的に所有し、支払先のアドレスに対して一義的に到達することが求められる。このような性質の実現可能性の程度については、仮想通貨のウォレットとコインの構成に依存する。

1. 分散型仮想通貨の価値の所在

ビットコイン・システムにおいては、公開鍵暗号が使われており、秘密鍵の持ち主が対応する公開鍵と紐付けられたコインを使用し、収益を得て、処分する権利を有している。すなわち、コインに対する所有権を保有する主体は秘密鍵に対する排他的なアクセスを有する主体のことを指す。

ビットコイン・システムの利用者は、ウォレットに秘密鍵を保管する。これを安全に管理することによって、コインに対する所有権を行使する。しかしながら、ネットワークに接続されたマシンにおいて、一般の利用者がウォレットを安全に管理することは必ずしも容易ではない(図表5)。

図表5　ウォレットとコインの紐帯関係



（出所）木下宏揚（2016b）

(1) ウォレット・クライアントの構成

ビットコイン・システムにおけるウォレット・クライアントの構成には、秘密鍵の所在によって複数の分類があり得る。木下宏揚(2016a)および木下宏揚(2016b)によれば、次の5つの構成に分類される。

①完全クライアント

完全クライアントとは、数十GBのビットコイン開闢以来のブロックチェーンをすべてダウンロードする方式のことを指す。インストール後に使用できるようになるまで時間が掛かるなど、利用を開始することは容易ではないが、フルノードとしてP2Pネットワークに参加し、構成要素の1つとしてネットワークを支える意味を有する。

②軽量クライアント

軽量クライアントとは、SPV(Simple Payment Verification)のことを指す。完全クライアントのようにすべてのブロックチェーンをダウンロードするのではなく、数十MB程度の各ブロックのヘッダーのみをダウンロードする。これによって、ある取引が正当なブロックに含まれているかどうかを少ない情報で検出することができる。

③サーバクライアント

P2Pネットワークとして動作する完全クライアントのサーバにクライアントとして接続する方式のことを指す。この場合、秘密鍵はクライアント側に存在している。取引の正当性を検証する方法は、軽量クライアントにおける方法と同様である。

④ブラウザベース

ウェブ上のサービスとしてウォレット・クライアントを提供する方式のことを指す。この構成においては、秘密鍵はサーバ上にあるので、ローカルなウォレットを安全に保たなくてもよい。この方式には、取引のプライバシーを向上させやすいという利点がある。しかしながら、サーバを信頼できることが前提となる。

⑤ペーパーウォレット

ペーパーウォレットとは、QRコードなどを用いることによって、秘密鍵を物理的な紙に印刷して保存する方式のことを指す。ネットワークを通した不正侵入などに対して安全であることから、高額のビットコインの保存に適しているとされる。概念的にはペーパーウォレットと同様のものとして、コールドストレージという方式もある。これは、ネットワークから遮断されたストレージに秘密鍵を補完する方法として、紙媒体の代わりに電子的な記憶媒体を利用するものである。

(2) 秘密鍵の保管方法

ビットコインウォレットは、ビットコイン自体を入れておくわけではなく、取引を行うための処理を行うクライアントソフトウェアとしての機能を有する。具体的には、所有しているビットコインの秘密鍵のコレクションを含むファイルを保持しているソフトウェアである。このように、ビットコイン・システムにおいては、秘密鍵が通貨の象徴的機能の一部を果たしているのである。ビットコインの秘密鍵に対応する公開鍵からビットコインアドレスを生成する過程を図表6に示す。

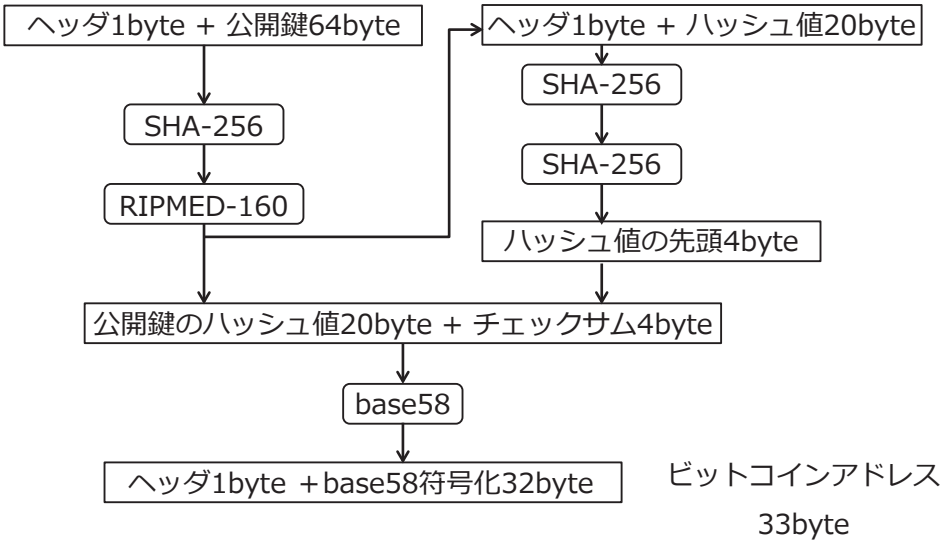
このシステムにおいては、コインに対応している秘密鍵を保持していることが、コインを行使する権利を保持していることになる。ビットコインウォレットには、ビットコインアドレスに対応する公開鍵と秘密鍵のペア、取引記録、取引の正当性を示すブロックチェーンの一部などが含まれている。

秘密鍵を保管する方式として、複数のウォレット・クライアントの構成が存在するが、いずれの方式においても完全なる安全性を確保することはできない。このことは、責任主体としての発行企業が存在しない分散型仮想通貨における安全性の課題であり、従って現時点においては、こうしたリスクを理解する利用者だけが決済手段として受容するもので

ある。

このように考えると、他に合理的な代替の決済手段が見当たらない国際間決済の一部の場面を除いて、分散型仮想通貨がキャッシュレス決済の方法として広く利用されることは現時点では想定しにくい。

図表6　ビットコインアドレスの生成



（出所）木下宏揚（2016b）

(3) 仮想通貨取引所における保管

およそ仮想通貨の保管というのは、ウォレット・クライアントを保有する秘密鍵の所有者の責任において行うべきものである。しかしながら、ネットワークに接続された環境においてローカルのソフトウェアを安全に管理することは容易ではない。また一方で、ブラウザベースのサービスを利用する場合には、ローカル環境の安全性に関する負担は減少するのに対して、サーバを信頼しなければならないという問題が生じる。

わが国においては、仮想通貨を個人がソフトウェアで管理する場面よりも、仮想通貨取引所に預託する形式をとる場合が多く見られる。この場合に、購入した仮想通貨を取引所に預けるというのは、厳密には何を預託するのであろうか。その具体的な内容については、預託の構成に応じて解釈することができる。

①利用者の請求権の内容

仮想通貨取引所に対する利用者の請求権の内容として、典型的には次の2つが想定される。

a. 法定通貨による払戻し

一定量の仮想通貨を取引所から購入し、仮想通貨の送付を受けることなく取引所に預託して、契約で指定した時点の交換レートで再び日本円に換算して日本円による払戻しを受ける内容である場合には、利用者は仮想通貨の秘密鍵の保管には一度も関与しない。

b. 仮想通貨による払戻し

一定量の仮想通貨を取引所から購入し、仮想通貨の送付を受ける場合には、秘密鍵の所在は利用者が選択するウォレット・クライアントの構成に依存し、秘密鍵を手元に置く場合と、ブラウザサービスのようにサーバ側に置く場合とがある。

②仮想通貨の保管の形態

仮想通貨取引所における保管の形態として、典型的には次の2つのパターンが考えられる。

a. 仮想通貨の個別保管

一定量の仮想通貨を取引所から購入し、これを仮想通貨取引所が個別のアドレスを設定して預かる場合には、これに対応する秘密鍵の所有者は秘密鍵に紐付く仮想通貨の保有者である。

この時、仮想通貨取引所は、個別の利用者から秘密鍵を預託されていると見ることができる。あるいは、個別の利用者のために秘密鍵の生成および保管を委任されたと見ることもできよう。

b. 仮想通貨の集合保管

一定量の仮想通貨を取引所から購入し、これを仮想通貨取引所が顧客グループのために設定したアドレスで保管する場合には、有体物でいうところの種類物に近いものであり、種類物の寄託契約に類似した状況となる。

この時、顧客グループのアドレスの秘密鍵を保有するのは仮想通貨取引所であり、すなわち取引所が顧客グループのために設定して保管する秘密鍵であると解される。

(4) 分散型仮想通貨のトランザクション構造

ここまで見てきたように、分散型仮想通貨を安全に保管し、あるいは預託するというのは、秘密鍵を安全に保管するということを意味する。そして、仮想通貨に対する排他的な占有権を表現するためには、秘密鍵の所有者の自由意思に基づく場合にのみトランザク

ションが発生するように構成されなければならない。これについて検討するために、分散型仮想通貨のトランザクション構造について確認する。

ビットコインの取引は、まず受領者のビットコインアドレスを支払者に送信し、支払者は受領者のビットコインアドレス宛てに送金を行う。取引の入力は支払い金額に応じて複数のビットコインを選択することもできる。入力するビットコインの合計金額は、1個のビットコインとして出力するか、2個の出力に分割する。

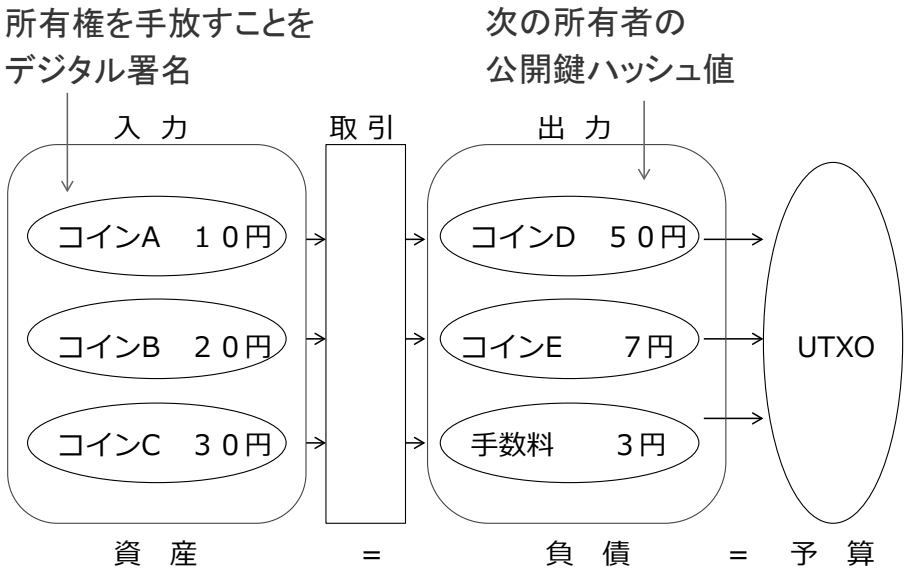
お釣りが必要な場合は、2個の出力のうち一方をお釣りとして自分宛てに支払い処理を行う。取引では、入力金額の合計＝出力金額の合計+取引手数料となる。取引手数料は、後述の採掘者への報酬として支払われる。今のところ、手数料はチップのようなもので義務ではない。

ビットコインにおいては、資産＝負債＝予算という等式が成り立つ。この表現方式のことを便宜的に時制的三式簿記と呼ぶことがある（図表7）。ブロックチェーンには未使用状態のコインが象徴的に存在している。この未使用状態のコインのことを、UTXO（Unspent Transaction Output）と呼ぶ。

ビットコイン・システムにおける前の取引記録とは、入力となるビットコインを受け取った取引で用いられたときの情報で、前の所有者がコインを現在の所有者に譲渡したという署名と現在の所有者の公開鍵のハッシュ値を格納している。この情報全体に、SHA256のハッシュ関数を2回適用したハッシュ値がPrevious Transaction Hashであり、これが前の取引の正当性を示す証拠の1つになる。

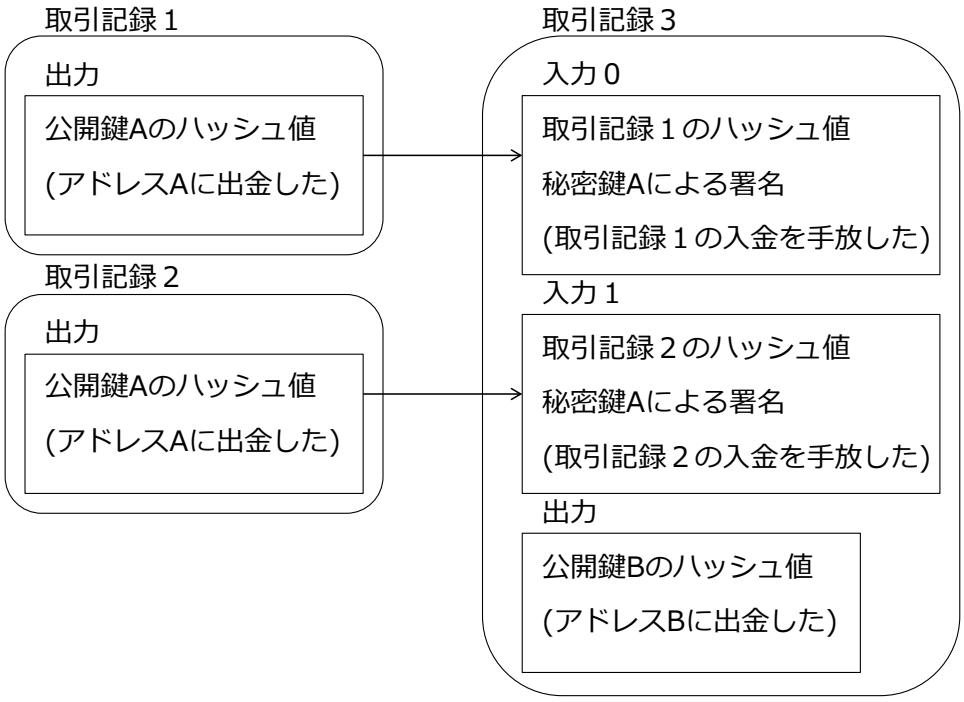
出力インデックスは前の取引の出力の何番目かを示している（出力が1つなら0番目）。署名スクリプトは、該当するコインを受領者への支払いに充てたことを示すための署名を格納する。トランザクション構成の例として、アドレスAからBへ取引1と取引2で入金したコインを、取引3として送金する場合の構成を図表8に示す。

図表7　ビットコインの時制的三式簿記



（出所）木下宏揚（2016b）

図表8　ビットコインの入力と出力



（出所）木下宏揚（2016b）

(5) 複数署名方式の適用

上記で確認したように、ビットコインを送金するというのは、自己の保有する秘密鍵によって取引記録の入金を手放すことを意味する。そのため、秘密鍵を保有する者がブロックチェーン上に記録された金銭価値に対する排他的な支配権を行使することができるが、不正なアクセスによって秘密鍵が失われた場合には、排他的支配権を失うことになる。

こうしたリスクを避けるために、複数の秘密鍵による署名がなければ入金を手放すことができないように設定する方法がある。この方式のことをマルチシグニチャーと呼ぶ。ビットコイン・システムにおいては、マルチシグニチャーは標準的な署名方法として技術文書に記載されている。

これを活用することによって、例えば利用者本人の秘密鍵および仮想通貨取引所の秘密鍵によって署名しなければ送金できないよう構成することができる。これは、秘密鍵を安全に保管することが難しいとされる個人のマシン環境の脆弱性を補う手法の1つである。しかしながら、仮想通貨取引所が何らかの理由で事業を継続できなくなった場合などに、複数署名の1つが所在不明となって送金ができなくなるといったリスクも内在する。

思うに、こうしたリスクを避けるためには、利用者本人、仮想通貨取引所、および監督官庁の3者がそれぞれ秘密鍵を保有し、これらのうち2つ以上の署名がなければ送金できないよう構成することが妥当である。これによって、仮想通貨取引所の事業継続リスクから利用者をある程度まで保護することが可能となる。

この手法を応用すると、監督官庁の保有する秘密鍵と仮想通貨取引所の秘密鍵をロックすることによって、利用者本人の保有する未使用残高を保全することが可能となる。同様に、監督官庁の保有する秘密鍵と利用者本人の秘密鍵をロックすることによって、仮想通貨取引所の保有する未使用残高を保全することが可能となる。これらは、緊急時における金銭的価値の保護や、あるいは破たん時における財産の差押えに代わる効果を有する。

複数署名による方式は、ビットコイン・システムなど一部の分散型仮想通貨には技術仕様として実装されているが、全ての仮想通貨に実装されているわけではない。これらの仮想通貨においては、未使用残高を保全するための代替的な手法を備えることが必要とされる。

2. 中央型仮想通貨の価値の所在

これまで分散型仮想通貨における未使用残高の保全方法について考察してきた。では、発行主体の存在する中央型仮想通貨においては、価値の所在はどのように理解すべきであろうか。

発行主体の存在する中央型仮想通貨においては、必ずしもブロックチェーン技術を適用することは必然的ではないため、特定信頼点を置いて一元的に残高を管理している場合があ

る。この場合には、各人の取引残高の根拠となるのは信頼できるサーバに記録された数字である。

中央型仮想通貨においても、ブロックチェーンもしくは分散台帳技術を用いて、分散型仮想通貨に類似した構成をとる場合もある。この場合であっても、特定信頼点である発行者が意思決定の主体となって、発行量の決定、および取引の監視を行うのであるから、未使用残高の保全は専ら発行主体の提供する手段の信頼性に依拠する。

米国における議論によれば、中央型仮想通貨を証券規制の対象とすることが検討されている。こうした規制手法を適用する場合には、監督官庁による取引の監視手法が存在することが発行の条件となるであろう。ブロックチェーンを用いて構成する場合には、秘密鍵の1つを監督官庁が保管する複数署名方式を適用し、中央型仮想通貨の発行主体もしくは仮想通貨取引所が不正アクセスを受けるなどのインシデントが発生した際には、監督官庁が未使用残高の移転を防止する策をとることができるように設計することなどが考えられる。

IV. キャッシュレス決済手段としての仮想通貨

本稿においては、仮想通貨がキャッシュレス決済手段の1つとして利用される可能性があるかについて検討した。そして、分散型仮想通貨におけるトランザクションの構造に着目し、未使用残高としてブロックチェーン上に表現された金銭的価値に対する排他的支配権の帰属について考察した。その結果、一般の利用者が日常的な支払手段として活用するためには、秘密鍵の保管に関する負担を軽減して安全性を高める方策が必要であることが導かれた。また、民間の仮想通貨取引所に保管の権限を集中させることは必ずしも適切であるとはいえず、監督官庁と仮想通貨取引所が協調的に複数署名のための秘密鍵を保管する方式が現実的であることを論じた。

本稿はまた、発行主体の存在する中央型仮想通貨がキャッシュレス決済手段として利用される可能性についても検討した。その結果、中央型仮想通貨は特定信頼点としての発行者が発行および流通を一元的に管理する仕組みであることから、金融機関ではない主体が発行者となる場合には証券規制の手法に準拠することが適切であることを論じた。なお、金融機関としての監督を受ける主体が発行者となる場合においては、発行主体の信頼性に関する議論を個別に行うべき必然性はなく、技術仕様の適切さに関する議論のみを行うことになる。

仮想通貨に応用されているブロックチェーンおよび分散台帳技術は、実用化が始まったばかりの段階にあり、さまざまな未知の論点が発見されている。さまざまな課題を発見して、改良のための方策を考案するために、複数の実証実験が実施されているところである。これらの実証実験を通じて、キャッシュレス決済手段としての仮想通貨の可能性についての議論が進展し、将来の可能性について有益な考察が加えられることが期待される。

参考文献

（邦語文献）

上杉志朗(2016)「仮想通貨の健全な発展について考える」『NEXTCOM』VOL.26, PP.14-23, KDDI総合研究所.

岡田仁志(2014)「ビットコインの構造と制度的課題―分散型仮想通貨の提起する論点とは」『情報処理学会誌』VOL.55, NO.5, PP.440-443.

岡田仁志(2015)「仮想通貨の登場が国家・社会・経済に与える影響」『電子情報通信学会FUNDAMENTALS REVIEW』VOL.8, NO.3, PP.183-192.

岡田仁志(2016a)「貨幣の歴史にみる仮想通貨の特異性―国家の通貨高権からCODEによる通貨発行へ」『NEXTCOM』VOL.26, PP.4-13, KDDI総合研究所.

岡田仁志(2016b)「ブロックチェインの分類に関する一考察」『ITUジャーナル』VOL.2016-9, PP.27-31.

岡田仁志(2017a)「ブロックチェーンが変える不動産登記の未来」『月報司法書士』特集：司法書士が抱える危険と対策, NO.546, PP.15-20, 日本司法書士会連合会.

岡田仁志(2017b)「仮想通貨に「信頼」は成立するのか―歴史から考察する「貨幣らしさ」の正体」『DIAMOND ハーバード・ビジネスレビュー』特集：ブロックチェーンの衝撃，2017年8月号，PP.56-70，ダイヤモンド社.

岡田仁志(2018)『決定版 ビットコイン＆ブロックチェーン』東洋経済新報社.

岡田仁志・高橋郁夫・山崎重一郎(2015)『仮想通貨―技術・法律・制度』東洋経済新報社.

岡本龍明・太田和夫(1991)『理想的電子現金方式』電子情報通信学会技術研究報告, 91巻127号, PP.39-47, 電子情報通信学会.

木下宏揚(2016a)「仮想通貨BITCOINを支える技術」『NEXTCOM』VOL.26, PP.24-33, KDDI総合研究所.

木下宏揚(2016b)「仮想通貨BITCOINを支える技術」『フィンテック：ブロックチェインの理解と応用』2016連続セミナー第6回(配布資料)情報処理学会.

経済産業省(2016)『ブロックチェーン技術を利用したサービスに関する国内外動向調査』.

山崎重一郎(2016)『FINTECHと金融サービスの将来像』福岡ブロックチェーンエコノミー勉強会資料, HTTPS://WWW.SLIDESHARE.NET/11RO_YAMASAKI/ (ACCESSED ON 31 DECEMBER 2017).

（英語文献）

BRACAMONTE, V. (2017), “THE ISSUE OF USER TRUST IN DECENTRALIZED APPLICATIONS RUNNING ON BLOCKCHAIN PLATFORMS”, PRESENTED AT THE IEEE 2017 INTERNATIONAL SYMPOSIUM ON TECHNOLOGY AND SOCIETY (ISTAS), (ON 10 AUGUST 2017).

BRACAMONTE, V., OKADA, H. (2017), “AN EXPLORATORY STUDY ON THE INFLUENCE OF GUIDELINES ON CROWDFUNDING PROJECTS IN THE ETHEREUM BLOCKCHAIN PLATFORM”, SOCIAL INFORMATICS, PROCEEDING OF THE INTERNATIONAL CONFERENCE ON SOCIAL INFORMATICS, OXFORD INTERNET INSTITUTE, UNIVERSITY OF OXFORD, PP. 347-354, SPRINGER.

BRACAMONTE, V., YAMASAKI, S., OKADA, H. (2016) “A DISCUSSION OF ISSUES RELATED TO ELECTRONIC VOTING SYSTEMS”, コンピュータセキュリティシンポジウム予稿集, 2C4-1, 情報処理学会.

OKADA, H., BRACAMONTE, V. (2016), “THE INFLUENCE OF THE EMERGING VIRTUAL CURRENCY ON NATION, SOCIETY, AND ECONOMY”, PRESENTED AT THE INTERNET, POLICY & POLITICS CONFERENCES (IPP), AT OXFORD INTERNET INSTITUTE, UNIVERSITY OF OXFORD (ON 23 SEPTEMBER 2016).

OKADA, H., YAMASAKI, S., BRACAMONTE, V. (2017), “PROPOSED CLASSIFICATION OF BLOCKCHAINS BASED ON AUTHORITY AND INCENTIVE DIMENSIONS”, PROCEEDINGS OF THE 19TH IEEE INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATIONS TECHNOLOGY (ICACT), PP.593-597.

UESUGI, S., OKADA, H. (2009), “DEVELOPMENT AND FUTURE USE OF PRODUCTION POSSIBILITY FRONTIER MODEL IN E-COMMERCE”, PROCEEDINGS OF THE ASIA PACIFIC CONFERENCE ON INFORMATION MANAGEMENT (APCIM), PP.253-260.

UK GOVERNMENT OFFICE FOR SCIENCE (2016), “DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN”, REPORTED BY THE UK GOVERNMENT CHIEF SCIENTIFIC ADVISER, UNITED KINGDOM.

YAMASAKI, S., OKADA, H., BRACAMONTE, V. (2016), “FEEDBACK TYPE COLLECTIVE INTELLIGENCE WITH NON-CONDORCET STYLE ELECTION SYSTEM USING BLOCK-CHAIN: APPLICATION TO SOCIAL INFRASTRUCTURE”, THE IEEE CONFERENCE OF NORBERT WIENER IN THE 21ST CENTURY, IEEE SOCIETY ON SOCIAL IMPLICATIONS OF TECHNOLOGY (SSIT), (ON 15 JULY 2016).