暗号資産の発行・取引と暗号資産交換業者のビジネスモデル

関西外国語大学英語キャリア学部教授・神戸大学名誉教授　滝川好夫

１　はじめに

暗号資産の１つとして、ビットコインを取り上げる。ビットコインの基本単位は１ＢＴＣであるが、ビットコインは小数点以下８桁まで分割することが可能であり、最小取引単位は０.０００００００１ＢＴＣ（１億分の１ＢＴＣ：１Satoshi）である。Satoshi はビットコインの考案者である「サトシ・ナカモト」に由来した呼び名である。

大塚[2025]は「（２０１０年５月２２日：引用者注）フロリダ在住のプログラマーが『ビットコインでピザを買いたい』とビットコイン開発者のフォーラムに投稿し、それに応じたピザ屋がいて、『ピザ２枚＝１万ＢＴＣ』で取引が成立します。それまでただのデータにすぎなかったビットコインが、はじめて現実のモノと交換でき、リアルに価値を持った瞬間です。」（p.145）と述べ、５月２２日が「ビットコイン・ピザ・デイ」と呼ばれていることを紹介している。ただし、私見では、これは単なる「物々交換にすぎない」と言うこともでき、ビットコインが「一般的」交換価値をもつようになったとは言えない。

大塚[2025]によれば、ビットコインの価格は「イメージとしては、マーケット参加者同士をネットワークで結んで売買している『ナスダック』市場に近く、証券会社に当たる取引所（暗号資産交換業者など：引用者注）のネットワークを通じて、ビットコイン価格（取引レート）がリアルタイムで決まっていきます。」（p.156）である。

本稿では、ビットコインの発行、取引（売買、送付・受取など）の実際のメカニズムおよび暗号資産交換業者のビジネスモデルを概説する。

２　ビットコインの利害関係者

大塚[2025]によれば、ビットコインの利害関係者を中心から列挙すれば、以下のものである。

① 開発者コミュニティ（コア・デベロッパー）

「開発者コミュニティ」はビットコインのソフトウェアを開発している。大塚[2025]はビットコインの価値はブロックチェーン技術の進歩しだいであり、「技術の成長に賭ける暗号資産投資で見るべき指標は、開発者コミュニティの盛り上がり（https://github.co.jp 参照：引用者注）です。」（p.91）と論じている。

② マイニング業者：マイナー、マイニング機器メーカー

ビットコインは、世界中で行われているビットコイン取引（移動：売買、送付・受取など）の承認作業の報酬として新規発行され、この新規発行が「採掘（マイニング）」と呼ばれ、採掘（マイニング）を行っている者は「マイナー（採掘者）」と呼ばれている。ビットコインの「マイニング業者」（例えば、ライオット・ブロックチェーンなど）は、スーパーコンピューター並みのマシンパワー（コンピューターの計算処理能力）と冷却装置を駆使して、電気代を負担して、およそ１０分ごとの最速承認作業を競い、勝者の報酬として、新規発行ビットコインを得ている。「マイニング機器メーカー」（例えば、Bitmain）はマシンパワーを生み出すための専用機械（マイニングに特化した集積回路（ＡＳＩＣ）を搭載した専用機械）メーカーである。

③ 取引所：交換業者、ＤＥＸ（分散型取引所）、ライトニングネットワーク（注１）

「交換業者」（暗号資産交換業者：Coincheck など）は中央集権型取引所（ＣＥＸ）であり、運営企業（中央管理者：Coincheck など）がビットコインの取引（売買、保管、送付・受取など）を行っている。「ＤＥＸ（分散型取引所）」（Uniswap など）は管理者が存在せず、ブロックチェーン上でプログラム（スマートコントラクト）によって利用者同士が直接取引を行っている。

④ サービス業者：レンディングサービス、ＥＣサイト、実店舗

ビットコインの「サービス業者」は、利用者が保有しているビットコインを「増やす」「使う」ための場を提供している事業者である。「レンディングサービス」は、ビットコインを貸し出して、利息を得るサービスである。つまり、それはビットコインを保有している利用者（最終的貸手）が一定期間「レンディングサービス」業者に貸し出し、業者はそれを他の利用者（最終的借手）に貸し出し、最終的貸手が利息を得るサービスである。（注２）「ＥＣサイト」（オンラインショップ：Shopify など）は、インターネット上でビットコインを用いて財貨・サービスを購入できるサービスである。「実店舗」（フィジカルストア）は、実店舗（ビックカメラなど）でビットコインを用いて財貨・サービスを購入できるサービスである。

⑤ エンドユーザー：サービス利用者、機関投資家、企業（事業会社）、個人投資家

３　ブロックチェーン技術と暗号資産の発行メカニズム

「ブロックチェーン」技術は「Ｐ２Ｐ（ピア・ツー・ピア）方式」を採用していて、ネットワークに接続されているコンピューター同士が直接データをやり取りできる。ブロックチェーンに参加している各コンピューター（「ノード」）は、他のコンピューターからデータを受け取る「クライアント」であり、他のコンピューターにデータを送る「サーバー」である。

ビットコインのネットワークに参加している「ノード」には、ビットコイン取引の過去の履歴の保存について、以下の２タイプがある。

① フルノード・タイプ

フルノード・タイプのコンピューター（「ノード」）は、ビットコイン取引の過去の履歴のすべて、つまり２００９年のビットコイン誕生時（ジェネシスブロック）から現在に至るまでのすべての取引データをダウンロードし、手元に保存している。

② 軽量ノード（SPV ノード）・タイプ

軽量ノード・タイプのスマホアプリは、各ブロックの「見出し」情報（木の「一番上の根（マークルルート）」）のみを保存し、ブロックの中身（ビットコイン取引の過去の履歴）を確認したいときは、フルノード・タイプのコンピューターに「私の取引は正しくブロックに含まれているのか？」と問い合わせ、フルノードから証拠（数個のハッシュ値（規則性のない、６４文字の英数字列）の連続：マークルパス）をもらうこと（「マークルツリー（ハッシュ木）」）で検証・確認をする。

ビットコインの取引（移動：売買、送付・受取など）は世界中で、１年３６５日、１日２４時間行われている。ビットコインの１つの取引は「トランザクション」と呼ばれ、「AさんからBさんへ・・ＢＴＣ移動する」という形で記録されている。記録はオープン（https://blockchain.com/explorer）であり、各取引は「Latest Transactions」としてネット画面においてリアルタイムで見ることができる。

大塚[2025]によれば、「ビットコインは特定の組織に属する開発チームで作られたものではなく、『サトシ・ナカモト』が公開した論文（“Bitcoin：A Peer-to-Peer Electronic Cash System”２００８年１１月：引用者注）に興味を持った人たちが分担してコードを書き、現在の形になりました。」（p.142）である。ビットコインは「ただのデータのかたまり」、ビットコインの発行は「マイニングによってビットコインを掘り当てた」としばしば言われるが、ビットコインの発行メカニズムの概略は以下の通りである。

（１） ビットコインはオープンソース・プロジェクトで開発されている。オープンソースは、プロジェクトはソフトウェアのソースコード（プログラムの設計図）を無償で公開し、誰でも「自由に利用できる」「中身を確認できる」「改良できる」「配布できる」、世界中の開発者が協力して品質を高めていくプロジェクトである。

（２）ビットコインは、ビットコイン取引（移動：売買、送付・受取など）の承認作業の報酬として新規発行される。この新規発行が一般には「採掘（マイニング）」と呼ばれ、世界中で行われているビットコイン取引の承認者は「採掘者（マイナー）」と呼ばれている。承認作業は、一般には「膨大な計算問題を世界中のコンピューターと競争して解く作業」と言われているが、それは詳細には以下の作業である。

ビットコインの各取引は、ネットワークに参加するノード（「マイナー」）によって検証・承認されてはじめて成立するものであり、（注３）ビットコインの多数の取引は約１０分ごとにまとめられて１つの「ブロック」を形成し、それが一括承認・検証される。新しく承認・

検証されたブロックは、これまでに承認済みのブロックを連結した「１本のチェーン（鎖）」（既存の一連のチェーン）の終端に組み込まれる。（注４）

以下では、「採掘者（マイナー）」のビットコイン取引承認作業（「マイニング」）を概説する。

１つ１つの「トランザクション」は「ハッシュ関数（ＳＨＡ－２５６）」によって「ハッシュ値」（規則性のない、６４文字の英数字列）に置き換えられる。（注５）「ＳＨＡ－２５６（Secure Hash Algorithm 256-bit）」はビットコイン取引で利用されている「ハッシュ関数」であり、それは入力されたデータを「ハッシュ値」と呼ばれる２５６ビット（６４文字の英数字列）の固定長データに変換するアルゴリズムである。ハッシュ関数は不可逆的、つまりいかなる大きさの入力データも「ハッシュ値」（規則性のない、６４文字の英数字列）に変換できるが、ハッシュ値から元の入力データを復元するのは不可能である。

ビットコインの各取引は、ブロックチェーン上で検証・承認されてはじめて成立するものであり、この検証・承認作業が「マイニング（採掘）」と呼ばれているものであり、それは以下の手順で、特定の条件を満たすハッシュ値を見つける作業である。

①　１つ１つのビットコイン取引（「トランザクション」）は「ハッシュ関数（ＳＨＡ－２５６）」によって「ハッシュ値」（規則性のない、６４文字の英数字列）に置き換えられる。およそ１０分ごとに、１つ１つのビットコイン取引のハッシュ値と、承認済みのブロックを連結した「１本のチェーン（鎖）」の終端にあるブロックのハッシュ値をひとまとめにする。

②　マイナー（採掘者）はひとまとめにされたデータ（１つ１つのビットコイン取引のハッシュ値と、ブロックチェーンの終端に位置するブロックのハッシュ値）に、「ナンス（Nonce）」と呼ばれる数字を付け加えて、「ハッシュ関数（ＳＨＡ－２５６）」によって「ハッシュ値」を求める。

③　マイニング（ビットコイン取引の検証・承認作業）を成功させるための条件は、生成されたハッシュ値の先頭に「ゼロ（０）」が２０個（ゼロの個数は採掘難易度が高まれば増え、低まれば減る）連続して並ばなければならないというものであり、そのために各マイナーは競って「ゼロ（０）」が２０個連続して並ぶハッシュ値を見つけるために「ナンス：Number used once」（３２ビットの値：「鍵」）を探す。（注６）

④　特定の条件を満たすハッシュ値を一番早く見つけた人がビットコイン取引の検証・承認作業（「マイニング」）の報酬として、新規発行ビットコインを得ることができる。

ビットコインの多数の取引は約１０分ごとにまとめられて１つの「ブロック」を形成するので、１時間で６個のブロック、１日で１４４個のブロック、１年で５２５６０個のブロックがブロックチェーンの終端に新たに組み込まれていく。

特定の条件を満たすハッシュ値を一番早く見つけた人がビットコイン取引の検証・承認作業（「マイニング」）の報酬として、新規発行ビットコインを得ることができる。

一般に「ビットコインの半減期」と呼ばれているものについて、下田[2024]は「ビットコインは一定周期で供給量が半減する『半減期』があらかじめアルゴリズムで決まっており、

需給関係がタイトになることを見込む投機的な資金が流れやすい構造にあります。」（pp.140-141]）と述べ、大塚[2025]は「ビットコインは４年に１回、マイニングの勝者に与えられる報酬が半分になると決められています（半減期)。」(p.188）と述べている。

以下では、「半減」についての「大塚 vs. 下田」について概説する。

（１）大塚[2025]の半減期

大塚はマイニングの報酬が４年ごとに半分になると述べている。ビットコインのマイニングは、およそ１０分間に１回行われる「取引の承認（１個のブロックの生成)」の競争であり、ビットコインのマイニング・ルール（アルゴリズム）は「１個のブロックはおよそ１０分ごとに生成され、ブロックが累計で２１万個生成されるたびに、１個のブロック生成当たりのマイニング報酬額が自動的に半分になる」というものである。１個のブロックが１０分ごとに生成されるので、２１万個のブロックの生成時間は、「２１万×１０分＝２１０万分」であり、「２１０万分÷６０分÷２４時間＝１４５８.３３日」「１４５８.３３日÷３６５日＝３.９９５年」であるので、約４年である。(注７）かくて、大塚の言う「マイニングの報酬（新規発行されるビットコインの量）が４年ごとに半分になる」というのは、具体的には、１ブロック当たりのマイニング報酬が以下のものであると注釈できる。

第１期（２００９年～２０１２年）　　５０ＢＴＣ
第１回半減期後（２０１２年～２０１６年）　２５ＢＴＣ
第２回半減期後（２０１６年～２０２０年）　１２.５ＢＴＣ
第３回半減期後（２０２０年～２０２４年）　　６.２５ＢＴＣ
第４回半減期後（２０２４年～２０２８年）　　３.１２５ＢＴＣ

（２）下田[2024]の半減期

下田はビットコインの新規供給量が一定周期で半減すると述べている。大塚の「マイニングの報酬（新規発行されるビットコインの量）が４年ごとに半分になる」というのは、４年ごとに、１個のブロック生成時に新規発行されるビットコイン量が半分になることを意味し、結局、大塚と下田は同じことを言っているのである。つまり、

第１期（２００９年～２０１２年）
　　５０ＢＴＣ×２１万ブロック＝１０５０万ＢＴＣ
第１回半減期後（２０１２年～２０１６年）
　　２５ＢＴＣ×２１万ブロック＝５２５万ＢＴＣ
第２回半減期後（２０１６年～２０２０年）
　　１２.５ＢＴＣ×２１万ブロック＝２６２.５万ＢＴＣ
第３回半減期後（２０２０年～２０２４年）
　　６.２５ＢＴＣ×２１万ブロック＝１３１.２５万ＢＴＣ
第４回半減期後（２０２４年～２０２８年）
　　３.１２５ＢＴＣ×２１万ブロック＝６５.６２５万ＢＴＣ

ビットコインの発行上限量は「サトシ・ナカモト」のソースコード（プログラム）におい

て２１００万ＢＴＣ（２０９９９９９９.９７６９・・・）であると規定され、発行上限の設定がビットコインをして「デジタル・ゴールド」と呼ばれている理由の１つである。（注８）

４　暗号資産の取引メカニズム

大塚[2025]は、暗号資産取引（ビットコイン取引）は「相対取引」である（p.156）と論じているが、預金が相対型取引であるのに対して、ビットコイン取引は「１対多数」「多数対多数」の市場型取引である。

パソコン・スマホは「さまざまな道具を入れる箱」であり、特定の作業を行うためのプログラム（道具）はパソコンでは「ソフト（ソフトウェア）」、スマホでは「アプリ（アプリケーション・ソフトウェア）」とそれぞれ呼ばれている。ビットコインの売買取引は、暗号資産交換業者（Coincheck, bitFlyer, GMO コインなど）の運営する、「サーバー（オフチェーン）」上のデジタル・マッチング・システムで、１年３６５日、１日２４時間行われている。（注９）

コインチェック株式会社共同創業者・大塚雄介[2025]は、ビットコインを手っ取り早く取引するには「暗号資産のアプリをインストールする」ことであると指摘しているが、それは次のことを意味している。

（１）「暗号資産アプリ」はビットコインを売買するための道具

「暗号資産アプリ」は、一般には「暗号資産交換業者アプリ（Coincheck アプリなど）」「ウォレットアプリ（自己管理型ウォレット：MetaMask など）」「情報・分析アプリ（CoinMarketCap など）」の３つの異なることを意味するが、大塚[2025]の「暗号資産アプリ」は「暗号資産交換業者アプリ（Coincheck アプリ）」のことである。

暗号資産交換業者（Coincheck など）は、ビットコインの「取引所サービス」「販売所サービス」「保管サービス」などを提供している。取引所サービスは、暗号資産交換業者がビットコインの売手と買手をマッチングさせるものであり、「板（オーダーブック）」を用いて、売手・買手同士の売買をマッチングさせるサービスである。販売所サービスは、暗号資産交換業者が提示している価格で、売手は暗号資産交換業者に売り、買手は暗号資産交換業者から買うサービスである。

暗号資産交換業者（Coincheck）のアプリを起動してログインすると、アプリ画面（iPhone/Android）の一番下に、４つのタブ（メニュー）、すなわち「販売所（暗号資産の価格一覧とチャート）」「ウォレット（現在の資産残高、入出金履歴など）」「ディスカバー（ニュースなど）」「アカウント（設定、FAQ、本人確認状況など）」などが並んでいる。

暗号資産の世界での「ウォレット」はビットコインを保管しておく「サイフ」であり、暗号資産交換業者に開設した「口座」である。Coincheck の「ウォレット」画面は「現在の資産（日本円、暗号資産など）残高の確認」「日本円の入金・出金」「暗号資産の送付（「送金」）・受取」「取引履歴の確認」を行うためのものであり、大塚[2025]によれば、Coincheck のアプリ画面（あるいはウェブサイト）を利用すれば、以下の操作で、ビットコインの売買・送

受金を行うことができる。

① 日本円を入金する：「ウォレット」画面

Coincheckの「ウォレット」画面で、まずは「日本円」→「入金」をタップする。ここで、「入金」ボタンのタップは「Coincheckへ入金するための振込先を確認するための準備」であって、実際の入金操作ではない。次に、「銀行振込」を選択し、画面に表示された振込先口座情報をメモ（またはコピー）する。最後に、取引銀行口座などからCoincheckの口座（振込先口座）へ振り込む。（注10）

② ビットコインを購入する：「販売所」画面あるいは「取引所」画面

ビットコインを「販売所」あるいは「取引所」で購入することができる。「販売所」で購入するときは、Coincheckのアプリ画面の一番下にある「販売所」をタップする。まず、コイン一覧から「BTC　ビットコイン」を選び、次に、「購入」ボタンをタップし、購入数量を入力する。最後に、「日本円でビットコインを購入」をタップし、「購入」を押す。たとえば、「１ＢＴＣ＝５００万円」のときに「０.００１ＢＴＣ」と入力すれば「５０００円」と表示されるので、それでよければ「購入」ボタンを押す。「取引所」で購入するときは、Coincheckのアプリ画面の一番下にある「アカウント」をタップする。（注11）メニューの中にある「ＦＡＱ」をタップし、さらに「三（メニューボタン）」をタップし、「Coincheck取引所」を選択する。そうすると「板（いた）」画面に移動するので、「現物取引」欄で注文価格をタップし、注文量を入力し、「買い」ボタンを押す。（注12）

③　ビットコインを売却する：「販売所」画面あるいは「取引所」画面

Coincheckで購入されたビットコインの大半は、Coincheckの管理している「コールドウォレット」に保管されている。（注13）コールドウォレットはインターネットから完全隔離されているので、保管されているビットコインは外部からのハッキングによって盗まれる危険度はきわめて低い。（注14）Coincheckのアプリ画面上の「ウォレット」には、購入したビットコインの残高が記録されているが、それは銀行の預貯金通帳に記載されている預貯金残高のようなものであり、データ上の記録（システム上の記録）にすぎない。

「ビットコインはウォレットに保管されている」としばしば言われるが、正しくは、ウォレットに保管されているのは「秘密鍵」であり、秘密鍵は「このビットコインは私のものである」と証明し、保有しているビットコインの「移動」（所有者の名前の帳簿書き換え）を実行するための「コード」（「電子印鑑」：変換作成された、非常に長くて複雑な、世界に一つだけの英数字列）である。（注15）したがって、「暗号資産交換業者Coincheckでビットコインを保有している」は、Coincheckが「あなたの秘密鍵（「コード」「電子印鑑」「電子サイン」）」をCoincheckのコールドウォレットに保管していて、「あなたの指示があれば、あなたの代わりに電子印鑑を押して（電子サインして）、所有者帳簿書き換えを行う」ことを意味している。（注16）

Coincheckで購入されたビットコインは「販売所」あるいは「取引所」で売却することができる。「販売所」で売却するときは、Coincheckのスマホアプリ画面の一番下にある「販

売所」をタップする。「販売所」では、ビットコインを Coincheck によって提示された価格で売却する。まず、コイン一覧から「BTC　ビットコイン」を選び、次に、「売却」ボタンをタップし、売却数量を入力する。最後に、「ビットコインを日本円で売却」をタップし、「売却」を押す。「取引所」で売却するときは、Coincheck のアプリ画面の一番下にある「アカウント」をタップする。メニューの中にある「ＦＡＱ」をタップし、さらに「三（メニューボタン）」をタップし、「Coincheck 取引所」を選択する。そうすると「板（いた）」画面に移動するので、「現物取引」欄で注文価格をタップし、注文量を入力し、「売り」ボタンを押す。

④　日本円を出金する：「ウォレット」画面

Coincheck でのビットコイン売却代金を出金するには、「銀行口座を登録する」と「出金申請する」の２つの手順を踏まなければならない。まず銀行口座を登録するには、Coincheck のアプリ画面の一番下にある「ウォレット」をタップする。「ウォレット」画面で、「日本円」→「出金」をタップする。「出金口座」項目にある「選択（または追加）」をタップし、「出金口座を追加」を選択し、銀行口座情報（銀行名、支店名、口座種別、口座番号、口座名義など）を入力する。２段階認証を行ない、銀行口座登録を完了する。次に、出金申請するには、Coincheck のアプリ画面の一番下にある「ウォレット」をタップする。「ウォレット」画面で、「日本円」→「出金」をタップする。登録した銀行を選択し、「出金額」を入力し、「出金申請を行う」ボタンを押す。２段階認証を行ない、出金申請を完了する。

⑤　ビットコインを送る：「ウォレット」画面

Coincheck で保有しているビットコインを他人のウォレットや他の暗号資産交換業者へ移動する（送る）には、「移動先（送り先）情報の準備」と「移動する（送る）」の２つの手順を踏まなければならない。（注 17）まず移動先（送り先）の「アドレス（ビットコインアドレス）」情報を入手する。（注 18）ビットコインアドレスは「1」（レガシー規格）、「3」（セグウィット規格）、「bc1」（ネイティブ・セグウィット規格）などの頭文字から始まる２６～６２文字の長い英数字列である。（注 19）次に、ビットコインを送るには、Coincheck のアプリ画面の一番下にある「ウォレット」をタップする。「ウォレット」画面でコイン一覧から「BTC　ビットコイン」を選び、「送金」（送付）ボタンをタップする。第１に「宛先を追加/編集」ボタンをタップし、「新規追加」を選ぶ。ラベルをつけ、受取人（送付先）のビットコインアドレスをコピー＆ペーストする。第２に受取人（送付先）情報の詳細入力を行う。つまり、画面をスクロールしながら、まず「送付先の取引所（暗号資産交換業者）名」または「プライベートウォレット」を画面（プルダウンメニュー）に出てくるリストから選ぶ。次に、「受取人」について、「本人」「本人以外（知人・法人など）」を選択する。最後に、受取人氏名・住所（本人以外の場合）を入力する。第３に「送金目的」（送付目的）を選ぶ。第４に「追加」ボタンをタップし、入力した送付先データを保存する。第５に入力内容を再確認する画面が出てくるので、「OK」をタップする。第６に「二段階認証コード（Google Authenticator などの６桁の数字）」を入力・送信し、Coincheck から登録メールアドレスに

送付されてくる承認メール内のＵＲＬをタップする。これで送付先の登録完了である。第７に「送金」（送付）画面の一番上の「宛先」をタップし、送付先を選択する。「送金金額」（送付金額：ＢＴＣの数量）を入力し、画面下部の「次へ」または「ＢＴＣを送金（送付）する」ボタンを押す。第８に「送金（送付）を確定する」をタップする。画面に「送金（送付）申請を受け付けました」が出てくるので、以上でスマホによるビットコイン送付操作の終了である。（注 20）

⑥　ビットコインを受け取る：「ウォレット」画面

ビットコインを受け取るには、Coincheck のアプリ画面の一番下にある「ウォレット」をタップする。「ウォレット」画面でコイン一覧から「BTC ビットコイン」を選び、「受取」をタップする。第１に「アドレスを作成」ボタンを押すと、ビットコインアドレス（「1」、「3」、「bc1」などの頭文字から始まる２６～６２文字の長い英数字列）が表示されるので、アドレスの右横にあるアイコンをタップして「コピー」し、アドレスを入力する場所（メール、LINE など）を長押し、「貼り付け（ペースト）」をタップする。第２に、コピーしたビットコインアドレスが現れるので、メールや LINE の「送信」ボタンを押す。第３に、Coincheck から「入金完了のお知らせ」の通知が来るので、「ウォレット」画面で現在の資産残高（ＢＴＣの残高）を確認すれば、ビットコインの受け取り作業は終了である。

５　暗号資産交換業者のビジネスモデル

暗号資産交換業者（Coincheck など）は、ビットコインの「取引所サービス」「販売所サービス」「保管サービス」などを提供している。取引所サービスは、暗号資産交換業者がビットコインの売手と買手をマッチングさせるものであり、「板（オーダーブック）」を用いて、売手・買手同士の売買をマッチングさせるサービスである。販売所サービスは、暗号資産交換業者が提示している価格で、売手は暗号資産交換業者に売り、買手は暗号資産交換業者から買うサービスである。

利用者は、Coincheck で以下のサービスを利用している。

①　日本円を入金する
②　ビットコインを購入する
③　ビットコインを売却する
④　日本円を出金する
⑤　ビットコインを送る
⑥　ビットコインを受け取る

以下では、利用者が上記の６つのサービスに対して、いくらの対価を支払わなければならないのか、逆に、Coincheck サイドからは、これらの６つのサービスを提供することによって、いくらの対価を得ることができるのかを概説する。たとえば、「手数料」「売買スプレッド」を除いて、「１ＢＴＣ＝５００万円」のときに５万円で０.０１ＢＴＣを購入する、「１ＢＴＣ＝１０００万円」のときに０.０１ＢＴＣを１０万円で売却すると計画したとしよう。

（注 21）

利用者の負担する手数料・売買スプレッドなど、銀行（例えば、三井住友銀行）と Coincheck の受け取る手数料・売買スプレッドなどは次のものであり、結果として、利用者の実際の支払い金額・受け取り金額は以下のものになる。

① 日本円を入金する

三井住友銀行から Coincheck へ５万円を入金するときには、利用者は三井住友銀行に「入金振込手数料」として２２０円支払わなければならない。

② ビットコインを購入する

「手数料」「売買スプレッド」を除いて、「『１ＢＴＣ＝５００万円』のときに５万円で０.０１ＢＴＣを購入する」と計画したが、Coincheck の売買スプレッド（手数料相当分）は利用者から見て、「購入時プラス５％、売却時マイナス５％」であるので、市場価格が「１ＢＴＣ＝５００万円」であったとしても、Coincheck の販売所での Coincheck 提示価格（５％上乗せ価格）は「１ＢＴＣ＝５２５万円」である。したがって、「『１ＢＴＣ＝５００万円』のときに５万円で０.０１ＢＴＣを購入する」と計画していた利用者は、実際には「１ＢＴＣ＝５２５万円」の Coincheck 提示価格で、５万円で０.００９５２３８BTC（５万円／５２５万円）を購入することになる。利用者は５万円でビットコインを 0.０１ＢＴＣ（５万円／５００万円）購入しようと計画していたが、実際には０.００９５２３８BTC（５万円／５２５万円）しか購入できなかった。スプレッドは、ＢＴＣ量では「0.０１ＢＴＣ－０.００９５２３８BTC=０.０００４７６２BTC」であり、「１ＢＴＣ＝５００万円」で評価すると、２３８１円である。利用者の保有しているビットコインの価値は４７６１９円（＝０.００９５２３８BTC×５００万円）であり、５万円からは２３８１円減額している。Coincheck の収入（スプレッド収入）は２３８１円である。（注 22）

③ ビットコインを売却する

「手数料」「売買スプレッド」を除いて、「『１ＢＴＣ＝１０００万円』のときに０.０１ＢＴＣを１０万円で売却する」と計画したが、Coincheck の売買スプレッド（手数料相当分）は利用者から見て、「購入時プラス５％、売却時マイナス５％」であるので、市場価格が「１ＢＴＣ＝１０００万円」であったとしても、Coincheck の販売所での Coincheck 提示価格（５%引き価格）は「１ＢＴＣ＝９５０万円」である。したがって、「『１ＢＴＣ＝１０００万円』のときに０.０１ＢＴＣを１０万円で売却する」と計画していた利用者は、実際には「１ＢＴＣ＝９５０万円」の Coincheck 提示価格で、０.００９５２３８BTC を９０４７６１円で売却することになる。スプレッドは、１ＢＴＣにつき、「１０００万円－９５０万円＝５０万円」であるので、売却する０.００９５２３８BTC については、「０.００９５２３８×５０万円＝４７６２円」である。０.００９５２３８BTC を保有していた利用者は「１ＢＴＣ＝１０００万円」で売却すれば９５２３８円得られるのに、実際には Coincheck 提示価格（５%引き価格）「１ＢＴＣ＝９５０万円」で売却せざるを得ず、９０４７６円しか得られない。「９５２３８円－９０４７６円＝４７６２円」がスプレッド（手数料相当分）

である。Coincheck の収入（スプレッド収入）は４７６２円である。

④ 日本円を出金する

Coincheck からビットコインの売却代金９０４７６円を三井住友銀行の口座へ出金するときには、Coincheck へ４０７円を「出金手数料」として支払わなければならない。結局、利用者は５万円プラス２２０円の元手で、９０４７６円－４０７円＝９００６９円を最終的に得ることになる。利用者の負担する手数料、売買スプレッドの合計額は「２２０円＋２３８１円＋４７６２円＋４０７円）＝７７７０円である。（注 23）

⑤ ビットコインを送る

Coincheck で購入したビットコイン０.０１ＢＴＣを Coincheck とは異なる暗号資産交換業者に送付するときには、「送付（送金）手数料＝０.０００５ＢＴＣ」がかかる。ビットコインの市場価格が「１ＢＴＣ＝５００万円」であれば、つまり５万円を送金するのに２５００円（＝０.０００５×５００万円）かかることになる。（注 24）

⑥ ビットコインを受け取る

Coincheck とは異なる暗号資産交換業者からビットコイン０.０１ＢＴＣを Coincheck に送付してもらい、受け取るときには、Coincheck サイドの「受取手数料」はゼロである。

６　おわりに

本稿では、「暗号資産」としてビットコインのみを取り上げ、ビットコインの取引（売買、送付・受取など）の実際のメカニズムを Coincheck について調べた。いずれ「CBDC（中央銀行デジタル通貨 vs. ステーブルコイン」の対立軸の中で、ステーブルコインを検討したいが、本稿はその際のいくつかの検討課題を明らかにすることができた。

① ビットコインの価値はブロークチエーン技術の進歩しだいと言われているが、CBDC に対するステーブルコインの相対価値は、ブロークチエーン技術の進歩による、ステーブルコインの「安全性」「効率性」「利便性」の向上いかんであろうか。

② 暗号資産交換業者（Coincheck など）は、ビットコインの「取引所サービス」「販売所サービス」「保管サービス」などを提供している。ステーブルコインは暗号資産の一種であり、ステーブルコイン業者はどのようにして「取引所サービス」「販売所サービス」「保管サービス」などを提供するのであろうか。

③ 暗号資産交換業者（Coincheck など）の実際を観察していると、暗号資産（ステーブルコイン）の「市場」、「デジタル資産」の「デジタル」の意味、サイバー攻撃の問題が見えてくる。

④ 「暗号資産交換業者 vs. ステーブルコイン事業者」の対立軸で、ステーブルコインのビジネスモデルを比較検討しなければならない。

脚注

（注１）大塚[2025]においては、「ライトニングネットワーク」は取引所の１つとして挙げられているが、それは正しくは高速決済技術である。ライトニングネットワークは、ブロックチェーンの外に専用の通り道を作り、そこで何度もやり取りを行ない、その結果だけをブロックチェーンに記録する技術である。

（注２）「レンディングサービス」を提供している業者には、「暗号資産交換業者」（Coincheck、GMO コイン、bitbank、SBI VC トレードなど）と「レンディング専門業者」（PBR Lending, HashHub Lending, BitLending など）の２つがある。

（注３）ビットコインの各取引は、取引者がお互いを承認する構造ではない。取引者がお互いを承認する構造の一例は「ＩＯＴＡ（アイオタ）」であり、Ｍ２Ｍ（Machine-to-Machine）経済を想定して設計されたＩＯＴＡは、ブロックチェーンと同様に分散型台帳技術であるが、ブロックチェーン技術が１本の「チェーン（鎖）」、有料（マイナーへの承認作業報酬）であるのに対して、「タングル（Tangle）」と呼ばれている「網の目状」であり、無料である。

（注４）ビットコインの取引が多数であると、承認待ちの時間は長くなるかもしれない。このとき、承認待ち時間を短縮するには、トランザクションに手数料を上乗せすればよい。

（注５）「ハッシュ関数」は、入力データ・サイズの大きさのいかんにかかわらず、固定長データ（６４文字の英数字列）に出力変換するアルゴリズムである。６４文字は２５６ビットのデータ（２５６個の「０」あるいは「１」データ）を１６進数という形式で書き出したときの長さである。

（注６）「ゼロ（０）」が２０個連続して並ぶハッシュ値を見つけるために「ナンス：Number used once」（３２ビットの値：「鍵」）を探すことは「Proof of Work : PoW」と呼ばれている。

（注７）ブロックチェーンの運営は２週間に一度、マイニング（取引の検証・承認作業）の難易度を調整して「１個のブロック生成時間をおよそ１０分」にしようとしているが、実際の半減期は４年より数日早まったり、遅れたりする。

（注８）ビットコインの累積発行量が２１００万ＢＴＣに達した（２１４１年）あとは、マイニング（取引の検証・承認作業）に対する報酬は、ビットコインの新規発行ではなく、ビットコイン取引（売買、送付・受取など）の手数料によって行われると言われている。

（注９）ビットコインの取引は、最短で、１０分ごとにまとめて「ブロックチェーン（オンチェーン）」上のいわば「公の帳簿（分散型台帳）」に記録されるが、それまでの間は、リアルタイムで、暗号資産交換業者の自社サーバー（オフチェーン）内のデータベースで数字を書き換えるだけである。１０分間はブロックチェーン上での取引の承認を待つ最短時間である。

（注 10）Coincheck の「日本円を入金する」には「銀行振込」以外に、「クイック入金」「コンビニ入金」などがある。「クイック入金」（ペイジー決済）は、１年３６５日、１日２４時

間、即座に日本円を入金するサービスであり、Coincheck で「クイック入金」を申し込むと、「収納機関番号」（誰に支払うのか)、「お客様番号」（誰が支払うのか)、「確認番号」（セキュリィ用の番号）といった３つの番号が発行される。①銀行などの ATM から「日本円を入金する」ときには、トップ画面にある「税金・各種料金払込み」または「Pay-easy」のボタンを押し、画面の指示に従い３つの番号を順番に入力し、画面に表示される入金内容が正しければ「確認」ボタンを押し、「現金」あるいは「キャッシュカード」を選択し、入金する。②パソコン・スマホによるネットバンキングから「日本円を入金する」ときには、まず銀行アプリにログインし、「税金・各種料金払込み」または「Pay-easy」を選び、３つの番号を入力すると金額が表示されるので、そのうえで振込みを行う。「コンビニ入金」はコンビニ店頭で日本円を入金するサービスであり、Coincheck で「コンビニ入金」を申し込み、利用するコンビニを選択したうえで、入金額を入力する。画面上の「お支払い情報を発行」をタップすると、入金するための「バーコード」「受付番号」が表示される。コンビニの店頭で「バーコード」あるいは「受付番号」を提示し、現金で Coincheck 口座に入金することである。「クイック入金」「コンビニ入金」の問題点は手数料が高いことである。

（注 11）スマホアプリでの Coincheck「取引所」へのアクセスは「ホーム」画面のビットコインを選択し、下にスクロールするだけで「取引所（板取引)」へ行ける。

（注 12)「取引所」で「板」を見ながら売買するのであれば、スマホのアプリよりは、スマホの Web ブラウザ（iPhone ならば Safari、Android ならば Google Chrome といった Web ブラウザ）が、さらにパソコンの Web ブラウザが便利である。売買手数料は、取引所での売買が販売所での売買より安いが、スマホは販売所での売買、パソコンは取引所での売買に適している。

（注 13)「資金決済法」に基づいて、Coincheck で購入されたビットコインは「分別管理」されている。つまり、Coincheck 社の資産とは明確に分けて管理されている。

（注 14）購入したビットコインを自己保管する、つまり「ハードウェアウォレット」で保管するには、以下の作業が必要である。まずは、Ledger 社の Nano S Plus, Nano, Flex/Stax, Trezor 社の Safe3, Safe5 などのハードウェア（機器）を購入し、次に、メーカーの公式サイトから、購入したハードウェア（ハードウェアウォレット）に連動する公式アプリ（Ledger 社であれば Ledger Live、Trezor 社であれば Trezor Suite など）をダウンロード（インストール）する。ハードウェアはインターネットから隔離された形で、ビットコインを取引するためのいわゆる「秘密鍵（印鑑)」を保管するための機器である。

（注 15）ビットコインのコード（秘密鍵）は元を辿れば２５６個の「０あるいは１」が並んだデータ（２５６ビット）であり、１ビットは例えれば１個のスィッチであり、２５６ビットは ON, ＯＦＦのいずれかが２５６個並んだ状態である。２５６ビットは「２の２５６乗（１０の７７乗)」通りの数字列である。一般に「ビットコインの秘密鍵」と呼ばれているものは「２の２５６乗通りの数字列」を変換作成された、非常に長くて複雑な、世界に一つだけの英数字列である。「８ビット＝１バイト」であり、２５６ビットはデータ量で言う

と３２バイトである。1バイト（ビットを８個束ねたもの）はデジタルデータの基本単位であり、２５６ビットは８個ずつの束（バイト）にまとめると、３２個の束（３２バイト）になる。

（注 16）暗号資産交換業者（Coincheck など）のアプリ画面・Web ブラウザ画面（管理画面）のログイン・パスワードはアカウントに入るためのものにすぎない。「秘密鍵」の保管には次の３つがある。第１は安全重視のための暗号資産交換業者（Coincheck など）のコールドウォレット（ネットワークから完全隔離されたオフライン状態）である。第２は利便重視（即座の移動）のための暗号資産交換業者（Coincheck など）のホットウォレット（ネットワークに接続されたオンライン状態）である。第３は自己保管、つまり自ら「ハードウェアウォレット」を用意して自己管理することである。

（注 17）マネーロンダリング（資金洗浄）やテロ資金供与を防止するために、暗号資産を送る際に、送付人（送付元）と受取人（送付先）の情報を暗号資産交換業者（取引所）間で共有しなければならないという国際ルール（「トラベルルール」：日本では２０２３年６月から法律で義務化されている）があり、ビットコインを送るには、「誰へ（受取人の氏名）」「どこへ（送付先の取引所名）」「何のために（送付の目的：金融商品の購入、財貨・サービスの購入など）」などの情報を Coincheck のスマホアプリ画面で入力しなければならない。

（注 18）「トラベルルール」に従って、ビットコインを送るときには、受取人（送付先）に「誰へ」「どこへ」「何のために」などの情報を通知しなければならないが、日本の暗号資産交換業者（取引所）は２つの異なった情報通知システム（「TRUST」「Sygna」）を採用している。「TRUST（トラスト）」は Coincheck, bitFlyer, Bitbank, BITPOINT などによって採用され、「Sygna（シグナ）」は GMO コイン、DMM Bitcoin、楽天ウォレットなどによって採用されている。「TRUST」と「Sygna」は互換性がないので、相互のビットコイン送付は不可能であるが、SBI VC トレードなどは両システムに対応しているので、２つのシステムは SBI VC トレードを経由すれば相互送付は可能である。

（注 19）Coincheck で保有しているビットコインを他人のウォレットや他の暗号資産交換業者へ送るには、送り先の「アドレス（ビットコインアドレス）」情報を入手しなければならないが、高橋[2025]によれば、「ビットコインの場合は、原則１人１個のウォレットを持つところまでは（銀行口座と：引用者注）同じですが、送金先であるビットコインアドレスは無数に発行できるため、毎回違う番号（ビットコインアドレス）を発行して送金してもらうのが一般的です。つまり、１つのウォレットの中に無数のアドレスがある状態です。」（p.166）と述べている。

（注 20）スマホによるビットコイン送付操作の終了ののち、Coincheck による送付審査、ビットコインのネットワーク上での承認作業を完了ののち、送付先のウォレットに送付される。

（注 21）ビットコインの価格は「ビットコイン相場」「ビットコインと円の交換レート」と呼ばれている。大塚[2025]は、「ビットコインの価値は、国ではなく、それを支えるアルゴ

リズム（ブロックチェーン技術：引用者注）に対する信用で成り立っています。」（p.87）と述べている。そして、暗号資産の価格上昇の理由として、「ブロックチェーン技術の進歩」「法制度の変化（暗号資産に対する規制の整備）による市場参加者の増大」「マクロ経済環境の変化（インフレーションなど）」などを挙げている。

（注 22）ビットコインを「販売所」ではなく「取引所」で売買したときには、購入時・売却時のスプレッド（手数料相当分）はゼロである。

（注 23）本文はビットコインの市場価格が購入時は「１ＢＴＣ＝５００万円」、売却時は「１ＢＴＣ＝１０００万円」であるケースについての計算であるが、市場価格が不変であったとすれば、計算は次のようになる。「入金振込手数料＝２２０円」「購入時のスプレッド（手数料相当分）＝２３８１円」「１ＢＴＣの Coincheck 提示価格（５％引き価格）＝４７５万円」「売却代金＝0.0095238×４７５万円＝４５２３８円」「売却時のスプレッド（手数料相当分）＝２３８１円」「出金手数料＝４０７円」であるので、結局、利用者は５万円プラス２２０円の元手で、「４５２３８円－４０７円＝４４８３１円」を最終的に得ることになる。ビットコイン価格が変化しないとき、利用者は手数料、売買スプレッドなど５３８９円負担することになる。

（注 24）大塚[2025]は「国をまたいでお金を動かす手段として、ビットコインはすぐれています。なぜかというと、銀行を経由した従来の国際送金は時間もかかるし、送金手数料もバカにならないからです。（中略）『円→ビットコイン→ドル』『ドル→ビットコイン→円』のように、あいだにビットコインをかませるだけで、時間は大幅に短縮され、手数料も安くなるのです。」（p.162）と述べている。

参考文献

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic System", Satoshi@gmx.com.

大塚雄介『いまさら聞けない　ビットコインとブロックチェーン』（最新改訂版）ディスカヴァー携書、２０２５年９月。

下田知行『図解ポケット　中央銀行デジタル通貨（ＣＢＤＣ）がよくわかる本』秀和システム、２０２４年９月。