スマイル会資料

仮想通貨

２０１８．０４．２６

片岡康昭

１．歴史

２００８年「サトシ　ナカモト」の論文により仮想通貨の可能性が示された。サトシ　ナカモトは正体が不明で、２０１６年オーストラリヤの起業家クレイグ・ライトが自分がサトシ　ナカモトであると名乗り出たが、いまだ真相は藪の中である。一説によると「サトシナカモトはおよそ１００万ビットコインを所有しているため、正体がばれると課税される恐れがあるから名乗り出ないとも言われている。サトシ　ナカモトの名はビットコインの最小単位０．００００００００１ビットコイン（BTC）を１satoshi として残されている。最初のビットコインによる売買は、フロリダ在住のプログラマーがフォーラムに投稿し、ピザ屋がピザ二枚を１万 BTC で売ったことから始まる。５月２２日はビットコイン・ピザ・デイとして関係者のお祭りの日になっている。

２．技術的背景

仮想通貨の取引を行うコンピュータの環境は、通常のプロバイダを通した接続ではなく、ｐｅｅｒ　ｔｏ　ｐｅｅｒ（P2P）になっていて複数のコンピュータが互いに直接接続しており、一つの取引が行われると直ちにすべてのコンピュータにそのデータが送られて保存される。データは１０分ごとにまとめられ、これをブロックという。次の１０分間のデータがこれに続き、以後ブロックが鎖状につながっていて、これをブロックチェーンという。ブロックチェーンは取引データの帳簿でありこれが接続されているコンピュータに共有される。

１０分ごとにまとめたブロックが正しいものであるかどうかはコンペティションにかけられ、一番早く正しいことを証明したものに報賞が与えられる。これをマイニング（採掘）といい、ごく初期の段階では通常のコンピュータで処理できたが、規模が大きくなるに従い大型、高速計算機が必要となり、現在ではもっぱら中国の専門のマイナーがこれを行っている。

このようにして１０分ごとにビットコインが増えていくが、発行の上限は２１００万枚発行すると打ち止めになると決められており、２１４１年にすべてのビットコインが掘りつくされることになる。

ブロックの中身はトランザクション履歴で、取引データ、全ブロックのハッシュ値およびナンス値からなっている。取引はトランザクションと呼ばれ、すべてのトランザクションは

「Ａ氏からＢ氏にｘｘＢＴＣ移動するという形で記録される。Ａ氏がＢ氏にビットコインを売る（Ｂ氏がＡ氏から買う）場合もＡ氏がＢ氏にビットコインを送る（Ｂ氏がＡ氏から受け取る）場合にも、Ａ氏がＢ氏に何かの代金を支払う場合（Ｂ氏がＡ氏から受け取る）場合もＡ氏からＢ氏にｘｘＢＴＣ移動するという形で表現される。

ビットコインは仮想通貨であり、同じデータを使って二度目の支払いを行う（ダブルスペンディング）や偽のデータにより支払いを行うこと（偽造）を防ぐ必要があり、そのために暗号技術を使用している。具体的には、デジタル署名（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ）を使用する。ビットコインのデータはその所有者の署名がつけられていており、正しい署名ができる人だけが取引（次の人へのビットコインの受け渡し）を行うことができる仕組みになっている。送信者はビットコインのデータをもとに自分の署名をつけて送り、受信者はその署名が確かに送信者のものであることを確認する。これには以前「エニグマ物語」で紹介した素数を使用する秘密鍵と公開鍵を使用する技術が使用される。これによりビットコインを送ったのは確かに署名者であること（本人確認）、通信の途中で金額が変更されていないこと（改ざんの防止）、署名者はビットコインを送ったという事実を後で否定できないこと（否認の防止）といった点が担保される。

基本技術であるブロックチェーンは一定の時間の「取引の束」すなわちブロックを時系列でチェーンのようにつなげて記録していく。このブロックを参加メンバーがお互いに承認しあうことにより、データの改ざんによる偽造や二重使用ができない仕組みになっている。ビットコインの取引を書き込む「台帳」がチェーン状に連なっていくことからこのように呼ばれる。正当な所有者が受取人Ａと受取人Ｂの両方に同じコインを譲渡した場合（ダブルスペンディングのケース）にはどちらかの譲渡を正しい取引として決定する必要があり、これらを可能にするのがそれまでの正当な取引データを使って次の正当な取引データを承認するというブロックチェーンの仕組みである。

一つのブロックの中には①一定期間ごとの多数の取引データ、②前ブロックのハッシュ値、③ナンス値と呼ばれる数値の三つが含まれる。ナンス（ｎｏｎｃｅ）とはｎｕｍｂｅｒ　ｕｓｅｄ　ｏｎｃｅの意味で一度だけ使う使い捨ての数字で特別な意味はない。ただし、このナンス値によって次のブロックに使う「前のハッシュ値」が変わってくることがポイントになる。ブロック全体のデータは「前ブロックハッシュ値＋ナンス値」から構成されている。このうち「前ブロックハッシュ値＋取引データ」はすでに決まっているため、次のブロックに使うハッシュ値をコントロールするため、変えることができるのはナンス値のみとなる。ビットコインは次に新規ブロックを追加できる条件として「そのブロックのハッシュ値が一定の条件となることが必要」というルールが定められている。一定の条件とは具体的にはハッシュ値の最初に一定以上のゼロが続くことを意味する。このためこの条件を満たす適当なナンス値を探し当てる必要がある。

プルーフ・オブ・ワークはビットコインにおいて偽造や二重使用を防止するために取引を承認していく中心的な仕組みである。これはナンス値を計算することを意味する。具体的に

は「前ブロックのハッシュ値＋取引データ＋ナンス値」から新規ブロック用のハッシュ値を求め、そのハッシュ値の先頭に一定の数以上のゼロが連続して並んでいるようなナンス値を求めることを指す。ハッシュ値は一方向性の関数であり、出力値「ハッシュ値」から入力値「ブロック全体のデータ」を逆に計算することはできない。このためのプルーフ・オブ・ワークを行うためには、ナンス値に次々といろいろな数値を入れてブロック全体のハッシュ値を求めてみるという総当たり法により計算を行う必要がある。総当たり法では可能性のある組み合わせを片っ端から試してみることが必要で「力任せ探索」あるいは「しらみつぶし探索」と呼ばれる。このためには膨大な計算量が必要である。このような条件を満たすハッシュ値が求められ、新たなブロックが作成されることを「取引の承認」と呼ぶ。これによりそのブロックに含まれているすべての取引が承認され、取引が確定する。ビットコインではこの計算に約１０分を要するように設定されているため、１０分ごとに取引がまとめて承認されていく。悪意の攻撃者がビットコインを偽造しようとすると、ビットコインの偽造とはビットコインの取引データを改ざんすることなので、それに基づくハッシュ値が変わり、ナンス値を再計算しなければならない。また偽造したデータを正当なものとするためには次のプルーフ・オブ・ワークも計算し・・・・・・・という形で最新のブロックまで改ざんし続けることが必要になる。そのためには膨大な作業量が必要となり、世界中の計算者の計算能力をすべて合わせたよりも高い計算能力（コンピュータの処理能力）を持つことが必要となる。つまり、多数の善意の計算者がいる世界では悪意の攻撃者による再計算は正しい取引の承認のスピードに追い付くことはできず、偽造が極めて困難になるという仕組みになっている。事実、これまでハッキングによる盗難や、交換業者の不正な引出しといった事故は起きているが、偽造によるトラブルは一度も発生していない。

個々のトランザクションはハッシュ関数という特殊な関数によって規則性のない一定の長さの文字列（ハッシュ値）に変換される。ハッシュ関数にかけるとどれだけ大きなサイズのデータでも同じ桁数の全く異なる文字列に置き換えることができるので暗号技術でよく使われる。例えば、「Ａ氏からＢ氏に１ＢＴＣを移動する」という日本語の文字列をＳＨＡ２５６というビットコインで利用されるハッシュ関数にかけると「２Ｅ１Ａ…４８Ｅ６」という６４桁のハッシュ値が得られる。次に０を一つ加えて「Ａ氏からＢ氏に１０ＢＴＣ移動する」という文字列を同じＳＨＡ２５６にかけると「０Ｅ５Ｆ・・・・６８ＣＡ」という６４桁のハッシュ値が得られる。このように入力データをわずかでも変えると全く異なるハッシュ値が出てくるのがハッシュ関数の特徴である。そして入力データからハッシュ値を生成するのは簡単であるが、ハッシュ値から元のデータを割り出すことはできない。つまり不可逆的で、あとから勝手に変更できない。ハッシュ関数はハッシュ法で使う関数で、文字列（キーという）に対してデータの格納場所を示す関数である。一般的にはキーの集合のほうが格納場所よりも大きいので、異なるキーに対して同じ格納場所を与える可能性がある。ハッシュ法にはこの衝突に対する対策が用意される。

３．マイニングの仕組み

マイニング（ｍｉｎｉｎｇ）とはビットコインの取引に必要な計算を実行した人に一定のビットコインを付与する仕組みであるプルーフ・オブ・ワークを行って、あるブロックについて最初に最適なナンス値を求めた人に報酬として新にビットコインが発行され支払われることをいう。つまり、新たなブロックができた瞬間にビットコインが新規発行され、支払われる。通貨としてのビットコインの新規発行はこのマイニングを通してのみ行われる。見つかった回答が正しいかどうかは二番手以降の人たちがチェックを行い、複数の人が承認すればそのブロックは承認されてブロックチェーンの最後尾に追加される。ビットコインではマイニングの報酬を求めて一人一人の参加者が利己的に行動することが全体としてはビットコインの機能を正しく機能させ、全員の利益になるという巧妙な仕組みになっている。マイナーはそのために２４時間、３６５日せっせと大型コンピュータを動かして複雑な計算を行う。ビットコインは計算作業に基づいて新規発行されるため「特定の個人や機関の負債ではなく、また当局による裏付けもない」（国際決済銀行がない）という存在になっている。中央管理者がいない（中央銀行が存在しない）という点や、だれの負債でもないという点、そして計算に成功すると報酬として新規発行された通貨がもらえるという点など、ビットコインは通貨としては（仮に通貨とすると）かなり常識を破った存在といえる。その意味でビットコインは「通貨とは何か」という通貨の概念に再検討を迫ったものといえる。

４．ビットコイン類似の仮想通貨

仮想通貨といえばビットコインと思われているが、世の中には１０００種以上の仮想通貨が存在している。これらビットコインに類似した仮想通貨をアルトコイン（ａｌｔｃｏｉｎ）と呼んでいる。これはａｌｔｅｒｎａｔｉｖｅ　ｃｏｉｎの略でビットコインを代替するコインといった意味を持つ。またビットコインクローンと呼ばれることもある。主な仮想通貨は図１のとおりである。
ビットコインの時価総額は図２、ユーザ数の推移は図３の通りで１ＢＴＣのビットコイン相場は図４のとおりである。主な交換業者の名前は図５に示す。

５．ビットコインの取引

ビットコインの取引を行うためには本人確認の書類の提出が必要である。初めてコインチェックのウエブサイトにアクセスすると、メールアドレスの登録が求められる。スマホの人はｉＰｈｏｎｅのＡｐｐＳｔｏｒｅやＧｏｏｇｌｅＰａｙからコインチェックのアプリをインストールする。メールアドレスを登録すると折り返し確認メールが届くので、それをクリックして本人確認画面にアクセスする。フエースブックアカウントを持っている人はフエースブックで登録することができるが、実際に取引を始めるには本人確認の提出が必要である。本人確認画面では住所、氏名、生年月日など必要事項を入力のうえ、運転免許証やパスポートなど本人写真入りの身分証明書画像（免許証の場合は住所変更の有無を

確認するため裏の画像も）と、提出された身分証と本人が一緒に写っている写真（写真入りの面を表に向けた免許証やパスポートを手に持った自撮り写真）を画面上の指示に従ってアップロードする。スマホの場合はその場で自撮りしてそれらの写真を送ることができる。登録後、しばらくすると「本人確認終了」のメールが届く。さらに数日後、住所確認のための書類が簡易書簡で登録住所に送られてくる。それを受け取り、登録住所が間違いないことを確認できたら登録完了でビットコインの取引を始めることができる。コインチェックのウエブサイト（またはアプリ）にログインすると「ウオレット」画面が現れる。この画面はいくつかのメニューが並んでいるが大きく①入金する、②出金する、③コインを買う、④コインを売る、⑤コインを送る、⑥コインを受け取るに分けられる。①入金は現金の出し入れに関するメニューで円やドルなどの現金を取引所の指定口座に預けておいて、その金額の範囲内でビットコインを買うことができる。預けた金額を証拠金としてレバレッジ取引をすることができる。②出金するは現金の出し入れに関するメニューでビットコインを売った代金を受け取りたいときは銀行口座を登録する。取引所に預けてある円やドルのうち現金で引き出したい金額を指定すると、その金額が銀行口座に振り込まれる。③コインを買うはビットコインの売買に関するメニューで、円やドルを支払ってビットコインを受け取ることをビットコインを買うといい、ビットコインを支払って円やドルを受け取ることをビットコインを売るという。「コインを買う」で買いたいビットコインの額を入力すると、必要な円が自動的に表示される。例えば１ＢＴＣ１０万円の時に０．１ＢＴＣと入力すれば１万円と表示され、これでよければ購入をクリックする。ウオレットで残高を確認すると、ビットコインが日本円に置き換わっている。コインを買うのオプションとして「クレジットカードで買う」方法もある。④コインを売るはビットコインの売買に関するメニューで、買ったビットコインはパソコンやスマホにダウンロードされるのではなく、コインチェックのサーバにおいてある。「コインを売る」画面で売りたいビットコインの額を入力すると、売却代金の日本円が自動的に表示されるので、その金額でよければ「売却する」をクリックする。⑤コインを送るはビットコインの送金と支払いに関するメニューで「コインを送る」のメニューを開く。ビットコインを送るには送る相手が指定したビットコインアドレスに送る方法と、相手のメールアドレスに送る方法がある。ビットコインアドレスは２７～３４桁のランダムな文字列で、送るたびに毎回別々のアドレスが発行される。ビットコインアドレスはＱＲコードで読み込むこともできる。⑥コインを受け取るは「コインを受け取る」のメニューを開くと入金用のビットコインアドレスが表示されるので、それを送ってくれる相手に知らせる。

６．ビットコインは通貨化か？

通貨であるかないかの議論において、法律的側面と金融的側面が考えられる。法律的な側面においては２０１４年「ビットコインに対する質問主意書」が出され、これに対する政府の答弁書；内閣総理大臣名では、我が国において通貨とは、通貨（コイン）について

は「通貨の単位および貨幣の発行等に関する法律」で額面価格の２０倍まで、日本銀行券については「日本銀行法」において無制限にそれぞれ「法貨と」して通用するものとされており、ビットコインは通貨に該当しない。民法における「通貨」とは強制通用力を有する貨幣および日本銀行券であって、これを用いた「金銭債務の弁済」が当然に有効となるものをいうと解されており、強制通用力が法律上担保されていないビットコインは当該通貨に該当しないと一刀両断にビットコインは通貨でないものと断定している。その理由付けとしては「法律で通貨と定めているものには含まれていない」ため、ビットコインは通貨でないという一種の同義語反復（トートロジー）的な説明になっている。後半の民法の部分についても強制通用力を持つものだけが通貨なのであるから「強制通用力が与えられていない」ビットコインは通貨ではないという、いわば定義により通貨でないという問答無用の説明ぶりになっている。この政府見解ではビットコインが果たしている機能やその性格に照らして、法律上どのように判断するのかという本質的な点については何ら判断が示されていない。一方では１０１７年４月に施行された「改正資金決済法」においては第二章で「仮想通貨」を不特定のものとの間で物品やサービスの購入に対する代価の弁済のために使うことができるとして定義されている。これは仮想通貨の役割から見て「通貨に準じた機能」を果たしていることを認めたものと解釈できる。２０１７年７月にはビットコインを含めた仮想通貨の購入時にかかっていた消費税が撤廃され、税制の面からもモノやサービスではないとされ、支払い手段としての位置づけがさらに明確になった。

「金融論」において貨幣（通貨）は①一般的な交換、②価値の尺度、③価値の保護手段という三つの機能があるとされ、これらを持っていればビットコインは通貨に該当することになり、そうでなければ通貨には当たらないことになる。第一に一般交換手段とは交換手段または支払い手段としての貨幣の機能で、世界で約９５００の店舗がビットコインによる支払いを受け入れており、ビットコインは広がりは限定的とはいえ、一般的な交換手段としての機能は備わっている。第二に、「価値の尺度」においてはインターネットのｅコマースのサイトで腕時計が０．８８１９２４ＢＴＣ、帽子が０．０２７７４２ＢＴＣなどと表示されており、ＢＴＣが価格を表示するために一定の機能を果たしていることがわかる。価値の保存は将来に備えて価値を蓄えておくことのできる機能で、ビットコインについていえばもともとビットコインが注目されるようになったきっかけは２０１３年３月のキプロス危機にあった。この時、キプロスでは銀行預金への課税や預金封鎖が検討され、これを受けて預金封鎖を嫌ったキプロスの資金（その多くはロシヤマネーとみられる）がビットコインに流出し、ビットコインの相場は１ＢＴＣ＝５ドルから２５０ドル以上まで一気に急騰した。また、ビットコインについてはすでに将来の値上がりを期待した「ビットコイン専用の投資ファンド」が作られている。これらのことから、ビットコインはそれぞれ限定的とはいえ機能的には通貨として一定の役割を果たしている。ビットコインの実際の利用状況を見ると、①一般的交換手段や②価値の尺度の利用は限定的で、③価値の保存手段としての利用が中心になっている。ある研究ではビットコインによって小口の受け

取りと支払いの両方を行っている「通貨ユーザ」のビットコイン保有量は全体の２%に過ぎない。これに対して「パッシブ投資家」すなわちビットコインの受け取りのみを行い、支払いを一切行っていない人と「マイナー」の保有量は５割以上を占めており、ビットコインを純粋に価値の交換手段として使っているユーザはかなり限定的と結論付けている。

７．ビットコインに関係する事件

① ビットコインが違法取引に使われた「シルクロード事件」

ビットコインの取引は１件ごとにだれでも見られる形でネットワークに公開されている。つまり、どのアドレスとどのアドレスがいつ、どのような取引を行ったかについてはネットワーク上で閲覧が可能で、だれでも見ることができる。ただし、ビットコインを使うのには個人情報を公開する必要がないので、特定のアドレスは特定の個人とは結び付かない。これは銀行券に印刷されている「記番号」とその銀行券の保有者の関係を特定できないのと似ている。この性格を悪用した事例としてシルクロード事件がある。「シルクロード」は米国で違法薬物などを不正に販売していたウエブサイトである。このウエブサイトはマリファナ、ＬＳＤ、ヘロイン、コカインなどの禁止薬物を手広く販売していた。また違法薬物の他にも盗まれた口座番号やクレジットカード情報、偽造免許証などありとあらゆる違法なものが取引されていた。シルクロードは２０１１年に特別な手段によってのみアクセスできる「深層ウエブ」に作られた。この闇サイトではビットコインが決済手段となっていた。２０１３年にＦＢＩがシルクロードの運営者であったロス・ウイリアム・ウルブリヒトを逮捕し、サイトは閉鎖された。これによりビットコインは違法取引に使用されるものとされ、ダーティなイメージがついた。

② マウントゴックス事件

マウントゴックス事件は日本で発生し外部からのハッキングによって同社が顧客から預かっていたビットコインが大量に喪失したと発表された。顧客分の７５万ＢＴＣと自社保有の１０万ＢＴＣが消失しこれは当時のレートで約４７０億円に当たる巨額なものであった。その後の警視庁の調べでハッカー攻撃により消失したといわれていたビットコインの大部分は、実は元社長のマルク・ガルブレスが外部の口座に送金するなどして横領していたことが判明した。ビットコイン取引所の盗難事件はマウントゴックス事件にとどまらず２０１６年８月に拠点を置くビットコイン取引所である「ビットフィネックス」で顧客の口座から１２万ＢＴＣ（当時の時価で７５億円）が盗まれる事件が発生している。これは外部からの不正アクセスによるものであった。また別の通貨では、２０１６年６月に投資ファンド「ダオ」がハッキングを受け、集めていたイーサリアムが流出した（６５億円)。これはダオ側のプログラムに問題があったとされている。このほか、ビットスタンプ（英)、ゲートコイン（香港)、シェイブシフト（スイス）などが被害を受けた。これらの事件はビットコイン自体が偽造されたり改変されたりしたわけではなく、ブロックチェーンやプルーフ・オブ・ワークなどのビットコインの仕組みが破られたわけではない。ま

た、ランサムウエア事件ではビットコインが愛用されている。

８．ビットコインの保有者

ビットコインの保有分布は図６のとおりである。ビットコインのウオレットは世界で約１６００万個、ビットコインのアドレスは約１９００万個が存在する。一見すると１６００万~１９００万人からなる大きなコミュニティができているように見えるが、詳しく見てみると必ずしもそうではない。保有するビットコインが0~0．００１ＢＴＣというほとんど残高のないアドレスが１１２３万個と全体の５９%を占めている。０．００１ＢＴＣというと１ＢＴＣ＝４８万円で計算するとわずかに４８０円に過ぎない。これに0．００1~0．０１ＢＴＣの１７%と０．０１~0．１ＢＴＣ１４%を加えると全体の９０%のアドレスで0．１ＢＴＣ以下の少額のビットコインしか保有していない。この理由は第一にこのアドレスにはビットコインとはどういうものかを試してみたいという人が作った「お試しアドレス」が相当数ある。第二に、ビットコインで取引を行うに際してはアドレスとその取引情報が全世界に送信されるため、プライバシー保護の観点から取引ごとにアドレスを変えることが推奨されていることである。一つのウオレットで複数のアドレスを作成することが可能で、このためビットコインで支払いをする際にはその都度アドレスを作って取引を行い、あとはそのまま放置してあるという「使い捨てアドレス」である可能性がある。これがウオレット数１６００万個とアドレス数１９００万個の差になっているものと考えられる。いずれにしてもこうした理由によりほとんど残高のないアドレスが全体の６割を占めている。これに対して、残高が１～１０ＢＴＣ（４８～４８０万円）相当のアドレスは４７万アドレスで全体の２．５%、残高が１０ＢＴＣ以上あるのは１４．８万アドレス、全体の０．７８%になっている。これらを合わせた６２万アドレス、全体の３．３%が保有額からみて本格的な形でビットコインを保有・利用している保有者と考えられる。ビットコインの保有状況を見ると残高が１０～１００ＢＴＣ（４８０～４８００万円）のアドレスが全体の２６%を保有しており、同様に残高が１００～１０００ＢＴＧのアドレスが２３%、１０００～１万ＢＴＣのアドレスが１%をそれぞれ保有している。これらの残高階層を合わせると、ビットコインの保有量は全体の９割を占めている。一方で、これらのアドレスの数は合わせても１４．８万アドレスと全体の０．８%に過ぎない。つまり、上位１%の人（アドレス）が全体の９割のビットコインを保有している。このようなビットコインの偏在は初期のマイナーに対する大盤振る舞いが大きな要因の一つになっている。初期には１回のマイニングに対する報酬が今の４倍あったほか、競合するマイナーも少なかったためパソコンで難易度の低い計算をするだけで簡単にリワードを得ることができた。ビットコインの導入からしばらくは１ＢＴＣは１ドルに満たない価値しかなかった。２０２０年５月に１万ＢＴＣでピザ２枚（２５ドル相当）を買った逸話が残っている（現在の価値で４０億円以上)。ナカモト氏はビットコイン初期からの採掘者で、一度もビットコインを使っておらず１００万ＢＴＣ（４８００億円）を保有している

と推測される。ビットコインの採掘者は個人のパソコンでもマイニングが可能であった。しかしビットコインのプログラムではマイナーが多くなるにしたがって採掘がだんだんと困難になるように設定されており、競争が激しくなる中で必要な計算力が急激に上がってきている。最近ではマイニング専用のコンピュータ設備を設けた大規模な「マイニングファーム」が大きな役割を果たしている。マイニングファームの上位１３社で世界のマイニングの約８０％のシェアを占めており、この上位１３社のうち１０社が中国のマイニングファームで、そのシェアは合わせて世界の６８％を占めている。このうちＡｎｔＰｏｏｌ社、ＢＴＣＴｏｐ社の２社が中国国内で約５割、世界で約３割のシェアを握っている。マイニングは大規模コンピュータ設備を２４時間、３６５日稼働させて大量の電気を消費するので、電気代の安い中国のプレゼンスが大きくなっている（日本１２円／ｋｗｈ、中国４円／ｋｗｈ）。このようなマイニングファームでは体育館のような広大な施設にビットコインのマイニングに特化した専用のハードウエアを大規模に備え、数百億円にも上る巨額の投資を行って大々的にマイニングを実施している。

９．ビットコインの売買の主体

世界のビットコイン取引所における取引シェアを見ると、ＯＫコイン（中国)、フォビ（中国）ＢＴＣチャイナという中国の３つの取引所における取引高が世界の全取引の９３％と圧倒的な割合を占めている。ビットコインの保有構造やマイナーの偏りとともにビットコインの売買を行う利用者の構造にも偏在がみられる。ビットコイン取引所は米国、欧州、日本、中国など世界各地に１００以上も設立されている。この中で中国元の取引が９４％と圧倒的で、米ドルは４％、ユーロ１％未満、円１％未満である。中国の取引所でのビットコインの売買高が急増したのは２０１５年８月の人民元の切り下げ以降である。この切り下げをきっかけに人民元の先安観が高まった。このため人民元を大量に保有していた中国の富裕層の間では人民元をドルなどの外貨に移す動きが広がった。しかし、中国では人民元の出入りに対しては厳しい資本規制が課されている。また、このような資本の流出につながる取引の広がりに対しては外貨両替に上限額を設ける、申請書の提出を義務付けるなど規制が強化された。こうした規制を回避する手段として使われたのがビットコインで、ビットコイン取引所に対しては規制が緩く、また外貨両替の規制の対象にもならなかったことから中国の富裕層は人民元をいったんビットコインに換えたうえで、あとでこのビットコインを必要に応じて米ドルなどの外貨に換える動きに出た。当局は２０１７年に入ってからビットコインの大手取引所の検査に着手し、外貨管理やマネーロンダリングなどの違法行為がないかを徹底的に調べたうえでビットコインの引き出しを当面凍結するという強硬な措置をとった。

１０．ビットコインにおける懸念

ビットコインにおいても長期的に見た懸念材料がある。その主なものは①ビットコイン

の発行上限と②リワードの半減期がある。①ビットコインの発行上限は２１００万ＢＴＣと決められており、ビットコインのプログラム内のコードであらかじめ設定されている。２０１７年８月において既に１６５０万ＢＴＣが発行済みとなっている。つまり発行上限のうちすでに７７％が発行済みとなっている。ビットコインの価格推移をみると、２０１１年春までは１ＢＴＣは１ドル以下の価格で２０１２年夏までは１０ドル以下で取引されていた。それがキプロス危機（２０１３年３月に銀行預金への課税案の発表）をきっかけに一気に 100 ドル近くまで跳ね上がり、その勢いのまま２０１３年末には一時１０００ドルの大台にまで上昇した。その後マウントゴックス事件（２０１４年２月）などを受けて２０１５年初めにかけて２００ドル台へと５分の１水準まで暴落した。２０１５年秋以降は中国からの資本逃避に用いられたことから相場は徐々に上昇したあと２０１７年に入ると急ピッチな上昇となり、２０１７年８月には４０００ドルを上回る水準まで達している。こうした価格の荷動きはビットコインの利用が徐々に増えていることに加えて供給量が制限されているという仕組みに人々が気付き、将来の需給のタイト化を見越した投機的な動きが広がっていることによるものとみられる。発行上限に達するのは２１４０年頃とみられている。ラストデイになるとマイニングに対して全く新しいコインが発行されなくなる。それ以降もブロックは記帳され続け、取引を続けることは可能であるが、マイニングに対する報酬は全く付与されない。そうすると取引を承認する役割を果たすマイナーたちにとって、マイニングを行うインセンティブが失われてしまうことになる。マイニングは事実上ビットコインを動かすエンジンになっているのでこのエンジンが止まるとビットコインの取引は承認されず取引ができなくなる。取引の承認がスムーズに行われなくなると価格の下落が止まらずシステムとして崩壊してしまう破滅的な状況が発生する恐れがある。②のリワードの半減によるマイニング業者の撤退懸念は、マイニングに対するリワードが約４年ごとに減らされる設定になっていることによる。ビットコインが初めて発行された時点ではマイニングに対するリワードは１ブロックごとに５０ＢＴＣに設定されていた。このリワードの額は新たに２１万ブロックが作成されるごとに半減していく仕組みになっている。このため２０１２年１１月にはリワードは２５ＢＴＣになり、２０１６年７月には１２．５ＢＴＣに減らされた。このリワードの半減期は約４年ごとにやってくる。２０１６年の半減期にはビットコインの価格が約６００ドルであったのでリワードは１５００ドル（約１５０万円）から一挙に７５０ドル（約７５万円）に減ったことになる。これから先もリワードは約４年ごとに半減期を迎え、２０２０年頃には６．２５ＢＴＣに、さらに２０２８年頃には１．５６２５ＢＴＣに半減することになっている。マイニングファームはビットコインのシステムを支えるためといった使命感からではなく、もっぱら報酬目当てなので採算が赤字になれば冷徹にマイニングから手を引く可能性が高い。他の仮想通貨（あるとコイン）のほうがマイニングの収益性が高くなれば、ビットコインを見限って他の仮想通貨のマイニングにシフトする可能性もある。

１１．ブロックサイズがもたらしたビットコインの分裂騒動

ビットコインは２０１７年８月１日に二つの通貨に分裂した。中国の関係者がビットコインを分裂させて新たな仮想通貨ビットコインキャッシュ（ＢＣＣ）を作った。この背景にはビットコイン取引の上限問題がある。ビットコインの取引データを入れる「ブロック」のサイズは最大１メガバイトと定められている。１０分ごとの取引データをこの容量に収めるためにビットコインの取引は最大でも世界全体で１秒間に７件しか扱うことができない。１日当たりでは６０万件である。取引量が増えて取引がこのブロックサイズの上限を上回り、取引の渋滞や承認の遅延が発生するようになった。このため未承認の取引が数万件にも上る状態が常態化するようになってきた。この対策のため、ビットコインの関係者はそれまで二つの陣営に分かれて論争を繰り広げた。一つは取引データ内にあるデジタル署名を分離して取引データを圧縮する「セグウィット」という機能を追加することにより、１ブロックの容量は変えずに１件ごとの取引データを小さくする（ブロックサイズを小さいままにする）という考え方であり、この一派は「ビットコイン・コア派」またはスモール・ブロック派」と呼ばれる。これに対して一定時間内により多くの取引を可能にするために必要に応じて大きなブロックサイズを認めていくべきとする一派は「アンリミテッド派」またはビッグ・ブロック派」と呼ばれる。アンリミテッド派ではブロックサイズを単純に増やすのではなく、時間帯ごとの取引量に応じてブロックサイズを決定していくという「可変ブロックサイズを」を主張する。また２０１７年に入ると両派の折衷案としてセグウィットを導入したうえでブロックサイズを２メガバイトに増やすという「セグウィット２ＭＢ」案が出され激しい対立が生じた。対立の溝が埋まらなかったことからビットコイン・コア派は見切り発車的にセグウィットを２０１７年８月１日に導入しようとした。７月下旬になって分裂回避のため関係者の間で妥協案が成立し、折衷案である「セグウィット２ＭＢ」案を採用することが決まった。これに反発したのがマイナーの大手のビットメイン社（中国）やヴィアＢＴＣ社（中国）で、セグウィットを採用されると自社のビットコイン採掘専用マシンが使えなくなることからセグウィット２ＭＢにも反対し８月１日にビットコインを分岐（フォーク）させて新にビットコインキャッシュ（ＢＣＣ）を創設した。新しく創設されたＢＣＣはセグウィット機能を持たず、取引量対策としてブロックサイズを８メガバイトにまで拡大した。分裂後の展開は第一の従来のビットコイン（ＢＴＣセグウィット機能付き）とビットコインキャッシュ（ＢＣＣ）の二つのブロックチェーンに分岐して別々に取引されることになる。二つの通貨はそれぞれ独立した通貨として別々の価格がついて取引され、仮想通貨取引所では新しいＢＣＣをアルトコインの一つとして取引する。第二に、旧ビットコインの所有者は同数のＢＣＣを得ることになった。日本の多くの取引所ではＢＴＣの保有量に応じて利用者にＢＣＣを割り当てた。ビットコインの分裂は株式分割に類似した仕組みなので通貨の価値は理論的には分裂後のＢＴＣとＢＣＣの価値に応じて分割される。実際分裂後はほぼＢＴＣ９割、ＢＣＣ１割といった割合となり、分割された形で価格形成が行われた。第三にどちらがメインのビットコインとして機能していくかはそれぞれの使い勝手の良さで決まってくるものとされ、ビット

コインの優位は揺るがないものと思われるが、ＢＣＣのほうが速く、安く取引できるコインとなればメインチェーンとなる可能性はある。この分裂騒ぎからビットコインの不確実性について見えてきたものとして、第一に、プログラムに従い整然と運営されているように見えるビットコインも運営を巡る主導権争いから逃れられない、第二に、今後もこのような分岐が繰り返される可能性がある、第三に、中央管理者が不在であるビットコインの特徴が弱点になりかねないことを露呈したことである。

１２．各国における行政府の介入

各国においてビットコインをはじめとする仮想通貨に対しての規制が続々と導入されている。我が国においては２０１７年４月に「改正資金決済法」が施行され、仮想通貨に対する規制が導入された。この背景にはＧ７サミット（２０１５年６月得る舞うサミット）において仮想通貨の規制に向けて適切な行動をとることが合意されたことによる。その趣旨は仮想通貨となる４つの条件が定義され、第一は、モノやサービスを購入する場合にこれらの対価の支払いとしてだれでも使用できる財産的価値があること、第二に、仮想通貨自体を不特定多数の人の間で売買できること、第三は電子的な方法によって記録されているものに限定され、円建てや外貨建てのものを除くこと、第四にコンピュータを用いて移転することができるものとなっている。この法律のポイントは第一に仮想通貨の売買を行う仮想通貨取引所を「仮想通貨交換業」として定義したうえで、一定の条件（資本要件、財産的基礎等）を課し、また登録制とした。第二に、仮想通貨交換業に対しては一定の業務規程を課すこととし、特に自己の財産と利用者の財産を分離して管理することが求められるほか、口座開設時には本人確認が義務付けられた。第三には金融庁の監督を受けることとし報告書の提出のほか立ち入り検査を受けることとなった。これによりマネーロンダリングや違法な送金などができにくくなった。中国においても当局によりビットコインへの規制が行われ２０１７年７月にＯＫコイン、フォビ、ＢＴＣチャイナの３大ビットコイン取引所への当局の立ち入り検査が入り、その結果これらの取引所からのビットコインの引き出しが数か月にわたって停止された。また、レバレッジ取引や信用取引など、少ない資金で多くのビットコインを取引する手法が全面的に禁止された。こうした規制強化の影響からそれまで全世界の９割以上を占めていた中国でのビットコインの取引量は２０１７年２月以降約１００分の１に劇的に減少した。

１３．ビットコインはバブルか？

ビットコインの価格は２０１７年になって４倍以上値上がりしている（８月現在)。バブルかバブルでないかは破裂してみなければわからないといわれているが、これまで速いピッチで一本調子で値上がりしていることは事実である。ビットコインは誕生してから数年は９０セントなど１ドルを下回るような価格で取引されていたが、２０１７年８月中旬には４０００ドル（ピーク時は２万ドル）を上回るような価格で取引された。ビットコイ

ンの相場を見る上で注意しなければならないこととして、株式におけるような投資指標がないことである。株式の場合にはＰＥＲやＰＢＲといった株価の尺度があり、株価が調整される。ビットコインの場合にはこのような指標がなく、割高に対する警戒感が出にくく「上がったら買う、買うから上がる」といった一方向の相場になりやすい。ＢＩＳの報告書（２０１５年）では「仮想通貨の本質的価値はゼロである」と断言しており、「その価値は将来的にモノや法定通貨に交換できる」という信頼のみに由来するものであるとしている。最近の理論的な研究でも①ビットコインの価格には投機的要素がかなり含まれている、②ビットコインの価格はバブルである可能性が高い、③ビットコインの基礎的な価値（ファンダメンタルバリュー）はゼロであると結論が出されている。

１４．過去のバブルからの教訓

１７世紀のオランダにおけるチューリップバブルは約３年間で終わり、また不動産バブル、株式バブル、国債バブル、美術品バブルなどいろいろあったが「バブルは毎回違う顔でやってくる」が特徴である。また一回のバブルを経た資産はしばらく警戒されてバブルになりにくく、目先を変えて別の資産バブルでやってくる傾向がある。そして専門家らしい人が現れて、値上がりを正当化するような理論を理路整然と唱えだした時が特に危ないとされている。仮想通貨のもう一つの気になる動きとしてＩＣＯの盛行がある。２０１７年６月にブロックチェーン関連のプロジェクトである「バンコール・プロトコル」がイーサリアを用いたＩＣＯにより３時間余りで１６７億円相当を調達したのがこれまでのＩＣＯの最高額となっている。ＩＣＯを行うのはスタートアップ期の企業であり、その内容は玉石混交でリスクは高い。

１５．次世代のコア技術となるかブロックチェーン

ブロックチェーンはかなり汎用性の高い仕組みであり、金融分野のほかにも流通、不動産、医療などの非金融分野にも活用できる。金融分野でも特に国際的な送金や証券決済について期待度が高く、すでに各国でいくつかの実証実験が行われている。金融界では「ブロックチェーンが主役になる」という認識が共有されつつあり、この技術をどの分野に応用していくかが中心的な課題になっている。ビットコインはあくまでもブロックチェーンの最初の実用例であって、特殊な適用例の一つに過ぎないとの見方に変わってきている。ブロックチェーンの応用分野は幅広い分野が想定され、このうち仮想通貨に応用する場合を「ブロックチェーン１．０」、仮想通貨以外の金融分野に応用する場合を「ブロックチェーン２．０」、土地登記、資産管理、商流管理、医療情報、選挙の投票管理などの非金融分野に応用する場合を「ブロックチェーン３．０」として分類される。ブロックチェーンは取引記録を鎖のようにつなげて管理する仕組みで、すべての取引履歴が記録された、いわば大きな帳簿になっている。そしてネットワーク内の参加者が各自の持っている帳簿を同時に書き換えていく形で所有権の移転が行われる。このことはネットワーク内の取引

参加者が所有権の記録を分散して管理できるようになることを意味する。このためブロックチェーン技術のことを分散型台帳技術」またはＤｉｓｔｒｉｂｕｔｅｄ　Ｌｅｄｇｅｒ　Ｔｅｃｈｎｏｌｏｇｙ；ＤＬＴと呼ばれることが多くなった。また、共通帳簿；Ｃｏｍｍｏｎ　Ｌｅｄｇｅｒとも呼ばれる。取引が行われ、それに伴う帳簿の変更が合意されるとそれがすべての参加者に送られ（ブロードキャスト)、一定の時間内にすべての分散型台帳が書き換えられる。この一定時間のことをレイテンシーという。ネットワークの参加者はノードと呼ばれる。従来金融機関の世界では、取引記録を「信頼できる第三者」（ｅｘ．民間銀行、中央銀行、証券決済機関など）が中央型帳簿を使って集中的に管理するのが一般的であった。これが分散型台帳を使って各ユーザが分散して管理できるようになれば金融取引を劇的に低いコストで、しかもリアルタイムで行うことが可能となる。つまり、中央型帳簿から分散型帳簿に移行することによりグローバルな送金システムの構築や決済インフラの革新につながる可能性がある。分散型台帳技術の特徴として①改ざん耐性、②可用性が高い、③低コストがある。①の改ざん耐性は仮に過去に行われたＴ個目のブロック内の取引データを改ざんしたとすると、変更したブロックの内容を示すハッシュ値が変わる。すると、Ｔ＋１個目のハッシュ値を計算しなおしてそれをもとにＴ＋２番目のハッシュ値を計算し、という形で現在までのすべてのブロックをすべて作り直す必要がある。それを正規のチェーンより早く現在のブロックを成立させなければならない。これは膨大な計算量となりかつ、自分以外のマイナーと合わせた計算能力を上回ることが必要となる。②の高可用性とは低障害性と同義で、ブロックチェーンではネットワーク上の多くのコンピュータが同じデータを持ち合っており、分散したデータを管理する。分散されたデータベース上に多くのデータが同時に存在するので、自然災害や停電、外部からのハッキングなどによりどこか一か所のデータが失われても他の参加者のコンピュータが動いていれば全体のシステムを維持することができる。③の低コストについては通常金融機関では取引や顧客に関する膨大なデータベースを維持しており、そのために大規模な集中管理センタを保持してセキュリティやバックアップに巨額の費用をかけている。分散型台帳に移行することにより、コンピュータリソースが少なくて済む分散型のコンピュータやデータベースで取引を行うことがで、さらに「ブロックチェーン技術」による堅牢性やセキュリティ機能によって関連する部分のコストを削減することができる。金融分野における具体的応用は国内送金、国際送金、クラウドファンディング、貿易金融、債券発行、証券プラットフォーム、シンジケート・ローン、コルレス銀行間のノストロ照合、金融機関の社内システムなどが挙げられる。この中で、特に実証実験が進んでいるのが①国際送金と②証券決済の二つである。①国際送金における応用としては、米国のリップル社を中心とするリップルプロジェクトがある。このプロジェクトには２０１６年に入ってから欧米やアジアの大手銀行が参加するようになっており、注目度が高まっている。我が国においてもリップルの仕組みを利用して海外送金とともに国内送金を含めて安価にリアルタイムで行おうとする「内外為替一元化コンソーシアム」」が発足しており、都銀、地銀、ネット

銀行など６０行以上が参加する一大プロジェクトになっている。証券決済における応用では、株式や債券といった証券の決済は、現状では多くの当事者が関係する複雑なプロセスとなっていてブロックチェーンを利用することによってこのようなプロセスを大幅に合理化し、コストを削減できると考えられる。米ナスダック、豪証券取引所（ＡＳＸ）、日本取引所グループ（ＪＰＸ）などがパイロットプロジェクトや実証実験などを行っている。この分野で世界をリードしているのはナスダックで、２０１５年１２月から分散型台帳技術を使ったパイロットプロジェクトを稼働させている。これはナスダックリンクと呼ばれ、対象は未公開株式市場の株式である。ナスダックリンクはこれまでシステム化が進んでいなかった未公開株式を対象として、分散型台帳に記録する形で発行や売買を可能にするものである。未公開株の新規発行や売買のプロセスについて、現物の株式の発行が不要になるほか、決済時間も短縮されるなど大幅な合理化とリスク削減ができる。これはスタートアップ企業である「チェイン社」との協力により同社が開発した「チェイン・コア」というブロックチェーン技術を使う。ここではカラードコインという手法が使われ、ビットコインに資産に関する情報を付加することにより様々なアセットを少量のビットコインとともに移動させる。ビットコインに色（情報）をつけることであらゆるアセットを表現し、その移転を行うことから「色のついたコイン」と呼ばれている。ゴールドマンサックスでも「証券決済のための暗号通貨」を考案し、２０１５年に特許を出願した。豪証券取引所（ＡＳＸ）ではコアサービス（中心業務）である上場株式の決算、決済業務にブロックチェーンを利用することを計画している。ブロックチェーンを導入するかどうかの正式な決定は２０１７年末と予定されている。日本取引所グループ（ＪＰＸ）でも２０１６年に証券決済への分散型台帳技術の応用に関する本格的な実証実験を行った。パートナーは日本ＩＢＭ、野村総合研究所、カレンシーポート社で日本ＩＢＭとはハイパーレッジャーファブリックを、野村総合研究所等とはイーサリウム系のブロックチェーンを使った実証実験を行った。香港証券取引所（ＨＫＥＸ）では２０１７年８月にブロックチェーンを使った未公開市場を開設する計画を明らかにしている。スイス証券取引所（ＳＩＸ）では２０１７年８月にブロックチェーン技術を利用したコーポレートアクションの通知サービスを提供する計画を発表した。「コーポレートアクション」とは株式の価値に影響を及ぼす企業の意思決定に関する情報のことを指し、通知される内容には配当、株式分割、株式併合、株式交換、第三者割当増資などが含まれる。これによってすべての関係者が同時に同じ情報を共有することによるコーポレートアクション処理の自動化、効率化を図る。香港証券取引所とＳＩＸの背後には米ナスダックの存在がある。金融分野でのブロックチェーンの活用を考えた場合、高いセキュリティを確保することが必要であり、何か問題が発生した場合には不正な取引を差し止めたり、不正な取引業者をネットワークから排除する対応をとることが必要となる。このためビットコインのようなオープン型の仕組みは難しく、クローズド型の仕組みがとられる。

１６．通貨の電子化は歴史の必然

世界の中央銀行においても分散型台帳技術の利用に向けて本格的に動き始めた。今や「中央銀行が自らブロックチェーンを使って電子的な通貨を発行すべきか」というのが政策的な議題となりつつあり、いくつかの中央銀行ではすでに実証試験を行うなど、この課題について積極的に対応する構えを見せている。このような分散型台帳技術を用いて発行される電子的な通貨は従来の方の電子マネーや電子現金と区別するために一般にデジタル通貨（デジタルカレンシー）と呼ばれる。また中央銀行が発行する点を強調して「中央銀行デジタル通貨」（セントラルバンク・デジタルカレンシー）と呼ばれ、あるいは法定通貨に対応して法定デジタル通貨と呼ぶ場合もある。公的デジタル通貨ではビットコインのＢＴＣのように独自の通貨単位を持っているのに対し、公的デジタル通貨ではドル、円などの各国の通貨単位を用いる。つまり、従来型の現金、預金と中央銀行デジタル通貨とは１：１の交換比率で交換される。このため仮想通貨のように交換レートが乱高下するとった問題は起きない。新しい技術の導入についてはこれまで比較的保守的なスタンスであった中央銀行がブロックチェーンを使ったデジタル通貨の実証実験に乗り出している。最も典型なのが「世界初のデジテル通貨の発行国を目指す」と公言して「ｅクローナ」の発行計画を進めているスエーデン中央銀行である。こうした変革に向けた競争を後押しする仕組みとして国際決済銀行（ＢＩＳ）がある。ＢＩＳはバーゼルにある国際機関であり、「中央銀行中の中央銀行」と呼ばれている。決済システムについては「決済・市場インフラ委員会」（ＣＰＭＩ）という常設の委員会が設けられており、日、米、欧などの先進国や中国、インド、ブラジルなどの新興諸国がメンバーになっている。ＣＭＰＩには各国中央銀行で決済システムを担当する局長レベルが出席して定期的に情報の交換を行っている。中央銀行が通貨の電子化を考えるきっかけとなったのは民間における電子マネーの導入の動きであった。一つはネットワーク型の電子マネーである「ｅキャッシュ」で、１９９９年にオランダのデジタルキャッシュ社で研究開発が行われた。もう一つは英国の銀行が共同で開発した「モンデックス」である。これはＩＣカード型の電子マネーであった。シンガポールでは世界初の「法定通貨電子化」が進められている。２０００年１２月に当時シンガポールの通貨発行主体であった「シンガポール通貨理事会」（ＢＣＣＳ）が２００８年までに電子現金を国内の法定通貨（リーガルテンダー）にするという計画を発表した。このプロジェクトは「シンガポール電子法貨プロジェクト」（ＳＥＬＴ）と呼ばれた。その後ＢＣＣＳは２００２年１０月に中央銀行である「シンガポール通貨監督庁」（ＭＡＳ）に統合されＳＥＬＴはＭＡＳに引き継がれた。ＢＣＣＳでは電子通貨を導入する理由として、現金のハンドリングコストを下げ、社会全体の決済の効率を高め、シンガポールのキャッシュレス化を進めることを挙げていた。この電子法貨構想は実現には至らなかったが導入コストなどのコストが関係していた。日本銀行ではシンガポールより前から電子現金について研究を進めていた。１９９０年頃から日銀の金融研究所において「電子現金プロジェクト」と名付けた基礎的な研究が行われた。暗号学者を招いて暗号理論の

基礎やｅキャッシュの仕組みを勉強することから始められた。この研究は「ｅキャッシュや最新の暗号技術を使えば中央銀号が電子マネーを発行することができるのではないか」という基本的な問題意識のもとで進められた。通貨の発行形態がその時々の技術に依存する以上、新しい技術ができればそれを利用した通貨が当然という考え方があった。現金の電子化の問題点としては現金の持つ「転々流通性」をどのように確保するかという問題で、個人などが受け取った現金をそのまま他への支払いに当てることができることである。このタイプの利用は「オープンループ型」といわれるが、中央銀行の手を離れたところで電子現金が次々に持ち主を変えていくことになる。このため途中で偽造や二重使用が行われた場合に発見が困難となる。これを防ぐためには例えば個人Ａから個人Ｂに電子現金が支払われる時点で中央銀行との間で通信を行い、本物であることを確認することが必要になる。このためには取引ごとにリアルタイムでの通信が必須となり、膨大な取引件数に対してこのようなチェックを行うと途方もないコストがかかる。スイカ（ＳＵＩＣＡ）やパスモ（ＰＡＳＭＯ）といった電子マネーでは利用者が店舗で利用するとそれをその都度発行体に戻すクローズド・ループ型の仕組みをとることによってこのジレンマを回避し、安全性を確保している。１９９６年にはＮＴＴとの共同研究の形で「ＮＴＴ－日銀金融研究所の電子現金実験システム」として一応の成果を見た。このように各国の中央銀行は「通貨の電子化に向けた、デジタル通貨の実現」に向けて一斉に研究や実証実験に動き始めている。今のところ先導しているのは英国のイングランド銀行、カナダ中央銀行、シンガポール通貨監督庁（ＭＡＳ）、スエーデン中央銀行などであるが、日本銀行でもすでに基礎実験を完了し、このほか米国のＦＥＤ、オランダ中央銀行、中国人民銀行、香港金融管理局などでもデジタル通貨について検討・実験が試みられている。

１７．中央銀行がデジタル通貨を発行する場合の考察

中央銀行マネーの形態としては「銀行券」と「中央銀行の当座預金」の二種類があり、中央銀行によるデジタル通貨を考える場合にはこの二つが検討の対象となる。分散型台帳技術を使って銀行券をデジタル通貨にすることは「物理的な分散システム」を「デジタルの分散型システム」に移行させることで親和性が高いように見られる。「中央銀行の当座預金」（以下中銀当預）とは民間の銀行が中央銀行に預けている預金で、この当座預金は銀行が他の銀行との間で大口の資金決済を行う際の「決済資金（セトルメント・アセット)」として使用される。中銀当預では中央銀行が中央銀行各行の保有している資金の残高を電子的な帳簿によりシステムで管理しているので、すでに電子的な中央マネーとなっている。これらの中央銀行のマネーの性格を考慮し、中央銀行がデジタル通貨を発行するとき、中央銀行が銀行券を電子化した形でデジタル通貨を発行する（現金型デジタル通貨）場合は中央銀行が公的な仮想通貨を発行することになり、中央銀行が発行主体として「公的なブロックチェーンのシステム」を運営することになる。ユーザはパソコンやスマートホンを使用してお互いにデジタル通貨をやり取りする。単位は円、ドルなどとなり、

現金と等価になる。この場合の問題点としてだれがマイニングを行うか、マイニングに対する報酬、取引各確定までに時間がかかるなどがある。また中央銀行から直接発行を受けたデジタル通貨を使い、個人や企業がだれとでも直接決済し、銀行の中抜きが起きる。また銀行の貸出業務にも影響する。銀行の中抜きを回避するものとしてデジタル通貨をまず中央銀行が民間銀行に発行し、それを民間銀行が企業や個人に対して発行するといった二段階に分けた仕組みのモデルも登場している。その典型的なものはＲＳコインで、中央銀行であるイングランド銀行（ＢＯＥ）とロンドン大学で検討され、２０１６年論文として発表された。ＲＳコインについては登場人物は①中央銀行、②銀行、③ユーザの三つの改装に分かれている（図７）。このうち中央銀行のみが「信頼される機関」であり、銀行とユーザは不正行為をする可能性があるとされる。銀行はミンテンツと呼ばれ、中央銀行の許可を得た先のみが銀行；ミンテンツとしての機能を果たすことができる（クローズド型)。またユーザとはＲＳコインを使って受払を行う個人や企業をいう。このモデルでは二段階に分かれた「二階層」アプローチを採用しているのが特徴である。すなわち、銀行は分散環境によりユーザの取引を記録する「下位レベルのブロックチェーン」を共同で運営する一方、中央銀行は銀行から下位レベルのブロックを受け取ってそれを「上位レベルのブロックチェーン」に入れることにより、中央銀行がＲＳコインを発行する一方で銀行（ミンテンツ）が取引用帳簿（トランザクションレッジャー）を管理するという形で両者の役割を明確に分けている。これにより中央銀行は通貨発行を集中的に管理できる一方、個人や企業による膨大な取引の管理や顧客の対応を直接行わなくてよい仕組みになっている。送金人は取引銀行からＲＳコインの「未使用証明書」を受け取ってＲＳコインによる支払いを行う。ユーザ間の取引は銀行と銀行の合意によって承認され、下位のブロックチェーンに入れられる。銀行では一定時間ごとに下位レベルのブロックを中央銀行に送り、中央銀行ではそれを基に上位レベルのブロックを形成する。これがメインのブロックチェーンとなる。このメリットはデジタル通貨の発行手続きに要する膨大な作業を中央銀行が負わなくて済む、仮想通貨における取引件数の上限の問題を解決できる、このシステムの全体のカバナンスも中央銀行が行えることなどである。中国の人民銀行のデジタル通貨「チャイナコイン」もＲＳコインと同様に二階層によるハイブリッド型のデジタル通貨を目指している。また、デジタル通貨に「追跡可能性」をつけることにより汚職を減らすことも目指している。

１８．仮想通貨の種類

２０１７年２月の時点でコインチェックで取引している仮想通貨は全部で１９種、すべて分散台帳技術のブロックチェーンを基にしている（図１）。一番流通している取引高が大きいのはビットコイン（ＢｉｔＣｏｉｎ）であるが、分散型契約情報プラットフォームのイーサリアム（Ｅｔｈｅｒｅｉｕｍ）とイーサリアム・クラシックや分散型アプリケーションプラットフォームのリスク（Ｌｉｓｋ)、文書管理プラットフォームのファクトム

（Ｆａｃｔｏｍ)、代替コイン：ＡｌｔＣｏｉｎのモネロ（Ｍｏｎｅｒｏ)、予測市場（賭け市場）のプラットフォームのオーガ（Ａｕｇｕｒ)、即時グロス決済システムのリップル（Ｒｉｐｐｌｅ)、取引を追跡できない完全な匿名性を実現したジーキャッシュ（Ｚｃａｓｈ）がある。これらを買っている人は技術を認め支援する人、投機対象として客観的に眺めつつ安値で買い、高値で売る金融商品として見る人がいる。リスクが高くても大きな成長を見込む分野として新しい仮想通貨に投資する人が多い。デジタルの世界は勝者総取り（ｗｉｎｎｅｒ　ｔａｋｅ　ａｌｌ）の法則が働いて、シェアトップのみが生き残れるとされてきたがブロックチェーンについては用途別の仮想通貨が横並びに普及していて、全体を繋ぐのがビットコインとなる可能性もある。ＩＳＯにおいて標準化の議論も進んでいる。第二位のイーサリアムは内部通貨であるイーサ（Ｅｔｈｅｒ）の時価総額は２０１７年2月時点で１０億ドルで、一位のビットコインの１６９億ドルに対して一桁小さい。三位のリップルは2億３８００万ドルでさらに一桁小さくなっている。イーサリアムにおいてA氏がB氏に不動産を売る場合、A氏が行政書士に不動産移転登記の書類を作成してもらい、法務局に提出、同時に買い手のB氏がA氏に代金を振り込んで移転が完了するという流れになる。この一連の手続きを全部デジタル化しようというのがイーサリアムのプラットフォームの考え方で、契約情報を分散型台帳技術で管理する。最近注目されているオーガ（Ａｕｇｕｒ）はブックメーカー（賭け屋）の仕組みをデジタル化したプラットフォームで、使用される通貨はリピテーション（ＲＥＰ）である。日本では賭博行為として禁止されているが欧米では一般的でブックメーカーでは競馬、ボクシング、サッカー、オリンピックの勝敗からアカデミー賞の受賞者、大統領選の結果に至るまであらゆる勝負事が賭けの対象となる。このブックメーカーが対象とする予測市場で掛け金を現金でやり取りする代わりに、デジタルチップでやり取りするのが基本的発想である。ブロックチェーンはすべての記録が残るので誰からいくら入金されたか調べればすぐわかり、オープンで透明性が高いので胴元が不正してもすぐにバレるところが賭け市場に向いている理由である。取引がブラックボックスになっていると賭けに勝った人にきちんと支払われているか、胴元が余分に懐に入れていないか確認する手段がない。例えば日本競馬会（ＪＲＡ）のテラ銭（取り分）は２５％と決まっているが本当に７５％が配当に回されているか一般の人には確認する手段がない。また国際送金に向いているので国外の賭けに安い送金手数料で参加できるメリットもある。ただしオーガのブックメーカー自体のサービスはいまだ登場してない。

１９．参考文献

いまさら聞けないビットコインとブロックチェーン　　大塚雄介　　（株）ディスカバー・トゥエンティワン

アフター・ビットコイン　　中島真志　　（株）新潮社

ビットコイン入門　　エコノミスト　　毎日新聞出版

現代数理科学辞典　　広中平祐　　（株）大阪書籍
朝日新聞