２０１４年度　日本大学卒業論文

山田正雄ゼミナール

暗号通貨

ビットコインは、通貨の未来を変えるか

日本大学法学部法律学科 4 年

峯村 泰暢

2015/01/30

はじめに

最近、キャッシュレス社会が促進されており、なるべく貨幣を持たずに決済をする人が増えてきている。それは、電子マネーやクレジットカードなどにより、達成されてきた。しかしクレジットカード、電子マネーについては、法定通貨の価値を後ろ盾に決済をしているというだけに過ぎず、クレジットカードそのもの、電子マネーそのものが通貨として価値があるとみなされていたわけではない。また、法定通貨自体も、ほとんどの国が管理通貨制度に移行した今、国の信用を後ろ盾として通貨として流通させているに過ぎない。

経済がグローバル化する現在でも、世界の決済通貨は依然として米ドルである。大量の現金を国際送金する場合はあまり問題にならない決済手数料が、少額決済において非常に多くのウェイトを占め、結果的に国際的な少額決済はあまり浸透していない。

その中で、P2P（ピアツーピア）という方法により決済を完了し、他の法定通貨を価値の後ろ盾としない「暗号通貨」が台頭してきている。「暗号通貨」は「仮想通貨」「デジタル通貨」また、「仮想貨幣」「デジタル貨幣」など多くの呼び方がある。この研究では、最も取引量の多いビットコインを例に挙げ、それらがどのような経緯で登場したか、そして「通貨制度」と「情報技術」という２つの面からビットコインをはじめとする暗号通貨が「通貨」として確立されているのか、また、それらが一時のバブルとして終わることなく、今後ひとつの価値を認められた通貨として世界に通用するためにはどのような課題があり、それらは解決できるのか、解決されるのであればどのような方法により解決されていくのかを検討する。

目次

１．今日の通貨制度

ビットコインの検討に入る前に、今日の通貨制度について検討する。

１－１．通貨とはなにか

通貨とは、「流通貨幣」の略称で、国家などによって価値を保証された、決済のための価値交換媒体である[1]。実体として銀行券や硬貨などの補助貨幣（現金通貨）の他に、定期預金（預金通貨）などがある。国内で流通している貨幣は「法定通貨」といい、その国の法律により強制通用力が与えられており、「法貨」と略される。

１－１－１．通貨の３要素

今日、通貨には明確な定義が存在しないが、通貨には①決済、②価値尺度、③価値保蔵の３つの機能があるとするのが定説である。なにかものを買ったり、借金を返済したりする際にその通貨を支払うことで決済を完了させることができれば、それは通貨ということができる。ただし、ある程度以上の範囲の経済取引の決済に一般的に使える必要がある。次に、何かの経済価値の大小を示すときに、価格や賃金、資産価値などを通貨単位で示すときには、通貨が価値尺度として機能しているといえる。最後に、経済活動によって生み出された価値を、ある程度の期間蓄えておくことも通貨に求められる重要な機能である。この価値保蔵の要求レベルは、4 つの段階にわけられる。1 つ目がある程度の目減りを覚悟した保蔵機能である。硬貨の重さそのものが価値を表していた時代は、その硬貨が摩耗することにより価値が目減りしていってしまった。2 つ目が名目価値を 100%保蔵したいという要求である。これは紙幣の誕生により達成されたが、インフレが起きると、通貨の実質的な価値が下がってしまう。3 つ目が実質価値を 100%保蔵したいという欲求である。銀行預金も通貨とみなすため、銀行預金につく金利がインフレ率と連動すれば、実質価値を 100%保蔵することが可能である。4 つ目が、価値を増やしながら保蔵したいという要求である。これは失敗して価値を失う可能性があるため、現状では全員が達成することは不可能である。

１－１－２．通貨の種類

通貨が持つべき 3 要素を備えたものは、法定通貨以外にもある。銀行等に預けた預金は預金通貨と呼ばれ、通貨とみなされる。また、企業が独自に発行するポイントプログラムで、発行業者以外の商品やサービスと交換できるものを「企業通貨[2]」と呼び、これらは決済手段を持つとして通貨とみなされる。更に、その資産をすみやかに売却して、対価を普通預金口座に振り込めるのであれば、一般的な決済手段であるとみなされる。この論理により、CP[3]・国債・外債・社債なども、「広義流動性」と呼ばれる通貨に含まれるものとして政府の統計に載っている。また、ある一定の地域やコミュニティ内において法定価値と同等の価値があるとして発行され使用される貨幣で

[1] デジタル大辞泉より

[2] 他のポイントとの交換ができず流動性を持たないものは通貨とみなさない。

[3] CP（commercial Peper）…企業が短期資金の調達を目的に、マーケットで割引形式で発行する無担保の約束手形。2002 年にペーパーレス化を実現する法律が施工され、現在では電子 CP が主流となっている。発行取扱業者を通じて発行されるディーラーペーパーと企業が投資家に直接販売するダイレクトペーパーがある。

ある「地域通貨」も通貨とみなされる。この他に、IMF[4]が発行する国際統一基準通貨として SDR[5]などがある。

１－１－３．わが国の通貨制度

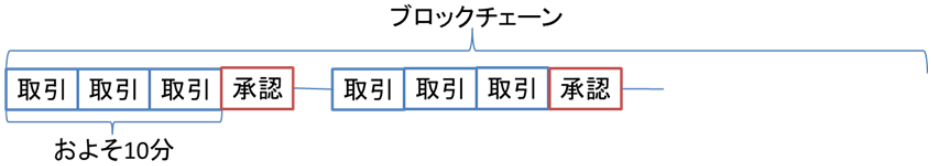
わが国の通貨制度に関する基本的な法律は「通貨法（通貨の単位及び貨幣の発行等に関する法律）」により定められている。これにより日本の法定通貨を「円」と定め、貨幣の種類は 500 円、100 円、50 円、10 円、5 円及び 1 円の 6 種類となっている。また、日本銀行法（平成 10 年 4 月 1 日施行）に基づき、わが国の中央銀行である日本銀行は日本銀行券を発行し、通貨として流通させている[6]。日本銀行券には日本国内で法定通貨として無制限に通用する強制通用力[7]が付与されている[8]。また、日本は 1931 年に金本位制[9]から管理通貨制度[10]へと移行した。管理通貨制度では各国の紙幣価値は金やドルではなくその国の信用が保証する。そのため、国の政治や建材が混乱することにより、紙幣価値が国際的に下がることになる。そのため中央銀行により、景気対策、物価調整、為替対策のための通貨量調整ができるようになっている。

２．ビットコインとはなにか

今日の通貨制度を見てきた。それでは、ビットコインとは何かという検討に入る。まず、ビットコインとはネットワーク上に存在する「暗号通貨（crypt-currency）」である。仮想通貨と表現されることが多いが、暗号によりコピー（偽造）を防ぐことで、電子データを通貨として流通させるシステムが根本にあるため、本検討では暗号通貨と呼ぶ。

4 IMF(International Money Fund)…国際通貨基金。為替相場の安定を図ることなどを目的に 1944 年に創設された。
5 SDR(Special Drawing Right)…IMF に加盟する国が持つ資金引き出し権、及びその単位。
6 日本銀行法 46 条 1 項
7 日本銀行法 46 条 2 項
8 無制限の強制通用力があるのはあくまで日本銀行券で、6 種類の効果については額面の 20 倍までが通用する（通貨法 7 条）。
9 発行する通貨の価値を金が保証する制度。各国の経済発展により、紙幣量が金の量を上回ったため、金本位制は維持できなくなっていった。
10 各国の中央銀行が、自国の経済規模に見合った分だけ通貨を発行する制度のこと。

２－１．ビットコインの仕組み



ビットコインは実体として硬貨や貨幣として存在せず、データとしてコンピュータの中にのみ存在する[11]単位の表記はBTC(ビットコイン)[12]。2014年9月8日現在1BTCはおよそ50224円である。ビットコインは、中本哲史と名乗る謎の人物の論文に基づき2009年に誕生した。コンピュータのユーザーどうしをP2P（ピアツーピア）でつなぐことにより、政府や中央銀行の規制を受けない「暗号化された通貨」を作り出すことができる。そしてその通貨はスマホやパソコン内の「デジタルウォレット」に保管される。取引内容はすべてブロックチェーン[13]に記録され、公開されている。また、取引は完全な匿名で行われる[14]。ビットコインは「マイニング」と言われる方法で生成される。マイニングは、ブロックチェーンが正しいかどうかを演算で求めることで、その報酬としてビットコインが支給される。ビットコインの総量は2100万BTCと定められており、流通量を制限することでインフレを抑える仕組みになっている。

２－２．ビットコインを支える技術

ビットコインは、コンピュータ上に記録されたデジタルデータを暗号化し、その「一意性」を保証することで、通貨になりうる属性をもたせたデータである。通常、デジタルデータのコピーは大変容易であるため、デジタルデータに通貨という属性を持たせることは難しい。紙幣などを物理的に複製するためには、物理的な条件を整えなければ複製が難しい手段で製造することによってある程度対処することができる。しかし、デジタルデータの複製は完全に防ぐことができない。この対策として、「暗号化」や「システム化」などの方法が取られてきた。暗号化とは複製したとしても正当な持ち主以外に読めなくするという方法であり、システム化とはデータの正当性を常に確認しながら動作するという方法である。ここでは、ビットコインがどのような技術によって支えられているかを見ながら、ビットコインが技術上安全なものであるかを検討する。

２－２－１．暗号化技術

ビットコインは、暗号化することで、取引する当事者だけが中身を読み取れるようになっている。暗号化はビットコインを始めとする暗号通貨にかぎらず、コンピュータを介したすべての取引を支えている。暗号化とは、ある数値を別の数値に変換する作業であり、それをもとの数値に戻す作業を復号化という。また、暗号化される前の文章を平文と言う。暗号化技術は共通鍵暗号が主流であったが、新しく登場した公開鍵暗号により、強固な暗号技術が確立された。

---

11 ただし、紙に印刷したペーパーウォレットを作成することができる。
12 表記のルールとして、IMFに承認されていない通貨をXから表すこととなっており、XBTと表記されることもある。
13 デジタル台帳。全ての取引記録が記録されたデジタルデータ。
14 ビットコインの取引で、互いに知りえるのは与えられた固有の文字列であり、ビットコインの所有者がだれかを特定することは不可能である。

２－２－１－１．共通鍵暗号

古くから使われてきた暗号方式は「秘密鍵暗号」と呼ばれ、ある特定のルールに則って文字や数字を別のものに置換する方法である。しかしこの方法では、秘密鍵を、情報を知ってもらいたい人に渡す必要があり、その過程で秘密鍵が他人に漏れる可能性がある。そのためどんなに難しい暗号を作っても、秘密鍵を狙われて突破されては暗号そのものの意味がない。そのため、現在では殆ど使われていない。

２－２－１－２．公開鍵暗号

現在使われている暗号技術は公開鍵暗号と言われる方式である。秘密鍵暗号では、暗号化に使われる鍵と復号化に使われる鍵が１つの秘密鍵であったのに対し、公開鍵暗号は１つの公開鍵と１つの秘密鍵を生成し、暗号化に使われる鍵と復号化に使われる鍵が対になっている。これにより、受信者が暗号化のために公開鍵を送信し、それにより暗号化したものを自身の秘密鍵で復号化するという方法である。により公開鍵方式のなかで最初に実用化された RSA 暗号を例に取り、実行例を挙げる。

２－２－１－３．RSA 暗号

まず、暗号化を行う前に予め以下の手順に従って秘密鍵と公開鍵を作成する必要がある。

１．２つの大きな素数ｐ，ｑを選択する。

２．ｎ＝ｐｑとφ(n)＝（ｐ－１）（ｑ－１）を計算する。 このｎを係数と呼ぶ。

３．Gcd（ｅ,φ(n)）＝１の関係をもつ乱数ｅ（公開指数）を選択する[15]。 ちなみに gcd とは２つの引数の最大公約数を意味する。 この公開指数ｅと係数ｎが公開鍵（ｅ,ｎ）となる。

１＝ｄｅ　mod[16]　φ(n)となるｄ（秘密指数）を計算する。 この秘密指数ｄと係数ｎが秘密鍵（ｄ,ｎ）となる。

４．公開鍵（ｅ,ｎ）を公開する。ｐ，　ｑ，ｄは誰にも知られないようにしておく。

RSA 暗号の原理は、平文を M、暗号文を C とすると以下の関係式が必ず成り立つという数学的特性を利用している。

$C = M^e \bmod n \cdots (1)$

$M = C^d \bmod n \cdots (2)$

（１）が暗号化の手順を示しており、（２）が復号化の手順を表している。ここで、暗号文 C と公開鍵を知っていたとしても、秘密指数 d の値を知らなければ暗号文 C から平文 M を得ることは計算的にほとんど不可能である。

実際の暗号化と復号化は以下のように行われる。A が B に対し重要書類 M を送りたいとする。まず、受け取り手である B が公開鍵（ｅ,ｎ）を A に送信する。この手段は特に規定されず、

[15] 一般的に、3 か 65537 が使われる。

[16] mod･･･モジュロ演算と呼ばれ、b=a mod n と表記した場合、「a は n を方として考えた時、b になる」という意味になる。つまり「a を n で割ったあまりは b である」ということである

鍵そのものが保証される方法であれば良い。次に A はその公開鍵を使い、（1）の計算式を使い平文 M を暗号化し暗号文 C を作成する。この暗号文を E メール等で B さんに送信する。A から暗号文 C を受け取った B は、（2）の計算式を用いて平文 M の内容を得る。

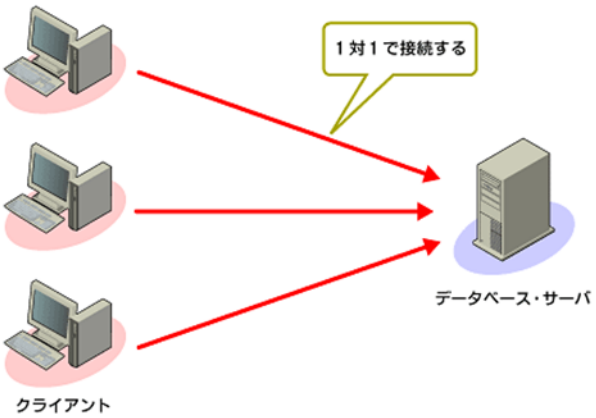
RSA 暗号は大きな数を素因数分解することが難しいという仮定と、暗号の式が一方向性であるという期待に基づいている。つまり、公開鍵暗号を解くことは理論上不可能ではないが、膨大な演算力[17]が必要であり、ムーアの法則[18]による演算速度の成長も RSA 暗号には追いつくことができないため、現実的には不可能であるということである。因数分解をすること以外で 2 つの素因数を見つける方法が見つかるか、量子コンピュータが登場することでこの暗号は突破される可能性があるが、現在両方共達成される見通しは立っていない。

２－２－２．ハッシュ化

ビットコインを支える暗号化技術をより強固にするために使われているのがハッシュである。ハッシュ[19]とは「内容が正しいことを示す符丁」のことである。ビットコイン・ネットワークは、取引情報を際限なく追記していく形で構成されている。そのため、取引情報は膨大な量になることが予想され、取引に遅延が発生する可能性がある。そこで、データ量を大幅に再現できるというメリットを持つハッシュを利用する。ハッシュを利用するにはあるデータを演算によりハッシュへと変換する（ハッシュ化）。この時、復号できない形で変換するのがハッシュの特徴である。このハッシュをブロックチェーンに組み込むことで、迅速な照会を可能にする。公開鍵方式の暗号化と、ハッシュ技術により、ビットコインはその一意性を保っている。

２－２－３．サーバークライアント方式とピアツーピア方式

ビットコインが他の通貨と本質的に違うところは、その決済や思想にピアツーピア方式を使用していることである。一般的な通貨や電子マネー、ゲーム内通貨などはどこかに「サーバー」が存在し、そこに「クライアント」が接続することで構成される。サービスを提供する母体を誰かが管理し、クライアントを利用する人々はそのサービスを享受するという形になっている。このため、消費者側の決済手続きを楽にすることで、年会費や決済手数料などの形で対価を得るビジネスにより提供されている[20]。しかし、ビットコインは管



17　2014 年現在、NTT はスイス連邦工科大学ローザンヌ校、ドイツ・ボン大学、フランス国立情報学自動制御研究所、オランダ国立情報工学・数学研究所との共同開発により、768 ビットの素因数分解を達成した。この演算には 4 年以上かかったが、これすら 1 例の秘密鍵を解読したに過ぎない（公開鍵方式には、取引の数だけ生成された秘密鍵が存在する）。また、現在は 1024 ビットまたは 2048 ビットの桁数の暗号が使われている。

18　「18 ヶ月で集積回路の演算技術は 2 倍になる」という法則。米インテル社の共同創設者の一人、ゴードン・ムーアが提唱した。素因数分解は、桁数が増えると飛躍的に演算力を必要とするため、演算力が RSA 暗号に追い付くことは現状ではありえないとされる。

19　「あるものを示すために使う短い符丁」を意味する。

20　決済手数料は原則として店側から徴収するが、それが価格に反映されていれば、結果的に消費者が負担していることと

理する主体がなく、ビットコインにかかわるネットワーク全体で支えられている。つまり、サービスを受けるデバイスが、同時にサービスを提供することにより管理コストを利用者全員に負担させているということになる。また、他の通貨のように発行を管理する主体（国家通貨で言うところの中央銀行）を持たないため、ビットコインの価値を意図的に操作したり、消滅させたりすることができない。

２－２－４．マイニング

発行主体を持たないビットコインは、マイニングという方法によって生成される。マイニングの本質は、ブロックチェーンの正しさを演算する作業である。一定時間中の取引情報をまとめたものをブロックと言い、前述のハッシュを鍵として鎖状になっている。これをブロックチェーンと言う。ブロックチェーンは、ハッシュの正しさが演算できるにつれ増えていく。ビットコインのシステムでは、最長のブロックチェーンを信頼することになっているため、もしブロックチェーンを偽造したとしても、鍵の正しさを証明する演算が正規のブロックチェーンより速い必要がある。しかし P2P 方式を採り、世界中の PC を並列処理させて演算している正規のブロックチェーンを追い越すことは理論上不可能である。これが、ビットコインが技術上安全であるという根拠である。マイニングには一定のマシンパワーが必要とされ、採掘量が増えるにしたがって要求されるマシンパワーは多くなる。すでに半分以上が採掘されている現状、１BTC を採掘するためのパワーは相当なものであり、一般家庭の標準的な PC では採掘が難しくなっており、一定のパワーを与えることで採掘時その分の報酬を得るマイニングプールが台頭している。このマイニングプールの台頭が、ビットコインの構造上の脆弱性に影響するが、これについては後述する。

２－２－５．取引所

ビットコインの元となった中本氏の論文には、ビットコインをドルや円などの通貨に換金する事に関する記述はない。また、ピアツーピア方式を採っているビットコインには、中心となる「サーバー」も存在しない。しかし、流通を促す「取引所」「換金所」が存在する。ビットコインには、「現金との交換を担当する仕組みが規定されていない」「決済を受け取る側で取引情報が確認されるまで最低 10 分かかる」という 2 つの欠点を持っており、それを補うのが「取引所」の役割である。取引所の役割は、マイニングに興味がなく、単にビットコインで決済や取引を行いたい人の代わりとして誕生した。利用者はまず取引所に「口座」を開設し、そこに自分のビットコインを蓄積しておく。他人にビットコインを渡す際には取引所を介して渡すことになる。これによりビットコインでの取引は上記の欠点から開放される。取引所は、それぞれの取引や換金について BTC で「手数料」をとり、それを収益源とする。ただし、その手数料は金額の 0.1%から 0.6%と、非常に少額である。

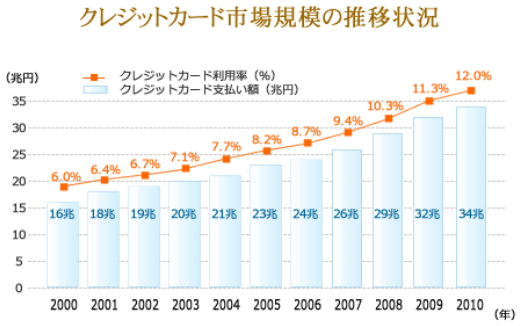
同義である。

２－３．ビットコインが登場した経緯

ビットコインはどのような需要に答えて生まれたのかを検討する。通常、通貨は色々な動機で保有される。1 つ目が取引動機で、想定内の買い物などの決済に使うために通貨を持つことである。2つ目が予備的動機であり、想定外の支出に備えて通貨を持つことである。3つ目が投機的動機で、資産をどのような形で保有するかを選ぶ中で、株や債券や不動産などではなく、通貨で持とうとすることである。多くの人がビットコインを使うようになった理由の第 1 は、国家通貨への不信であった。2008 年に起こったリーマン・ブラザーズの破綻を発端に世界的金融危機が発生したが、その際の自国通貨への不信が、ビットコイン保有の理由だった。第 2 に決済手段の利便性があり、とりわけ、国際・少額決済では取引コストの低さが際立っている。第 3 に投機対象としての注目がある。事実、登場当初は 100 円にも満たなかった 1BTC は、2013 年 11 月に 12 万 1501 円まで上昇した。その後も乱高下を続けたが、投機目的での資産の価値は十分にあったといえる。しかし第 1 の理由と第 3 の理由は誕生した結果そのような需要が生まれたのであって、ビットコインが登場するための需要は第 2 の理由、取引動機を背景としているとかんがえる。そこで取引動機に注目しながらビットコイン登場の経緯を検討する。

２－３－１．クレジットカード

昔から、決済には現金や小切手が使われてきたが、現金には高額取引に向かないという欠点がある。また、米国では高額紙幣の信用が低く使用が難しい[21]ことなどが契機となり、クレジットカードが登場した。クレジットカードは、利用できる加盟店で、商品の購入に際しクレジットカードを提示すると、いったんクレジットカード会社が加盟店への支払いを肩代わりし、後でカード利用者へ代金を請求する仕組み（ポストペイ型）となっている。現金を持たずに決済でき、盗難や不正使用による損害には保険が掛けられていることが多いため、現金より安全な決済方法として広く使われている。日本でのクレジットカード使用額は 2000 年に 16 兆円だったが、オンラインショッピング市場などでの決済の便利さにより 2010 年には 34 兆円と倍増した。しかし民間消費支出に占める割合は 12%にとどまり、クレジットカード利用先進国といわれるアメリカ合衆国の 24%やイギリスの 25%に比べ、かなり低い数値になっている。



２－３－２．決済サービスの多様化

現金に代わる決済方法として大きなシェアを占めるものは、長らくクレジットカードのみであったが、近年、非接触 IC カードの技術確立により、さまざまな方法での決済方法が可能になった。クレジットカードの技術を流用して作られるオンライン方式の電子マネーや、非接触式 IC

[21] 米ドルは米国内において法律上の強制通用力を持つが、実際に高額紙幣は偽造が多く、使いづらい。

カードを使って、店舗にある決済端末により決済を完了するオフライン方式の電子マネー、仮想クーポンとしてコンピューターネットワーク間取引だけで利用する仮想マネーなどである。とくにオフライン方式の電子マネーは、最初は各企業の囲い込みのため登場した背景があり、通貨とは呼べないものが多かったが、現在では各カード間の連携が取られるなど、単なる決済手段としてではなく、１つの通貨として認められるような成長を遂げている。ただし、これらはあくまでも決済サービスとしての多様化であり、通貨そのものが変化したわけではない。政府統計においても、電子マネーのほとんどは商品券として存在するということである。

２－３－２－１．電子マネー

２－３－２－１－１．オンライン方式

金融機関、クレジットカード会社または電子マネーのサービス会社のホストコンピュータと小売店等の決済用端末をオンラインで接続し決済を行う方法。クレジットカードと似た技術のため、既存インフラを参考にし、または流用しやすいメリットが有る。

２－３－２－１－１－１．PayPal

世界 190 カ国、23 通貨、2 億人以上が利用しているオンライン方式の電子マネー。オークションサイト eBay の子会社で、PayPal のアカウントを通して決済するため、よくわからない相手や会社に口座番号やクレジットカード番号を知られるのを敬遠する人に喜ばれた。また、国際郵便や小切手換金手数料などはだいたい 2,000 円程度かかるが、PayPal の場合は手数料がかからないため、海外取引を頻繁に行うオークションにはぴったりの電子マネーとなった。2011 年の総取り扱い数は 1180 億米ドル[22]。店舗側のスマートフォンやタブレットのイヤホン端子にスキャナーを設置し画面でサインをして決済したり、スマートフォン GPS で場所を把握、チェックインを実行することにより決済できたりする「PayPal Here」というサービスを開始するため、日本ではソフトバンクを筆頭株主とする合弁会社「PayPal Japan」が 2010 年に設立された。

２－３－２－１－２．オフライン方式

金銭価値を情報機器や記録媒体に置き換え、磁気カードや IC カードなどに収納し、小売店等の決済端末によりオフライン決済を行う方式。セキュリティの麺から、非接触型 IC カードによるものがほとんどである。日本で「電子マネー」というとこの方式が主流で、２０１１年度の主要６社 の電子マネー決済総額は２兆円を超えており、発行は１億７０００万枚を突破した。

２－３－２－１－１．技術仕様

サイズは長編が 85.6 ミリ、短編が 54.0 ミリｍ厚さが 0.76 ミリである。これは、磁気カードや接触型 IC カードの「ID-１ (ISO/IEC 7810)」という仕様に準拠している。非接触

22 日本円にして、11.6 兆円（2013 年 4 月）。

IC カードは約 0.2 ミリのシートを 4 枚貼りあわせた形になっており、IC チップとアンテナコイルが搭載されたシートと厚みを調整するシート（インレットシート）をカードの表面と裏面が印刷されたシート（オーバーレイシート）でサンドイッチにしている。非接触式 IC カードの電力は、リーダ／ライタから発信される電波を使って発生させる。ほとんどの非接触型 IC カードのカードでは電磁誘導方式を採用している。簡単に FIGURE4 に示したが、まずリーダ／ライタ（下の黒い端末）が磁界を発生させ、それに IC カードカード内のアンテナコイルが反応し電流を起こす。その電流が IC チップを作動させ、自分の情報をリーダ／ライタへと送り返すという仕組みである。情報を受け取ったリーダ／ライタはネットワークを通じてサーバーにアクセスし情報を確認、決済を行う。つまり、IC カードの情報自体を書き換えることによって金額を増やしたり減らしたりは不可能ということになる。非接触 IC カードの規格には、国際規格 ISO/IEC 14443 がある。非接触 IC カードは 13.56MHz の周波数帯を利用し、212kbps～847kpbs の速度で通信を行う。密着型・近接型・近傍型・遠隔型の 4 種類に区別され、さらに近接型は Type A と Type B に分類される。欧州では Type A カード、特にオランダのフィリップスエレクトロニクスが開発した MIFARE が普及している。米国ではモトローラが開発した Type B カードも普及している。ソニーは自社が開発した FeliCa を Type C として ISO/IEC 14443 に提案したが採用されず、後に FeliCa と MIFARE の上位通信方式が ISO/IEC 18092（NFC, Near Field Communication）として標準化された。

日本の規格として、JIS X 6321－6323 がある。として住民基本台帳カード仕様（Type B）、日本鉄道サイバネティクス[23]協議会による FeliCa の技術を採用した IC カード乗車券規格（サイバネ規格）などが普及している。

２－３－２－１－２．Suica（交通系電子マネー）

JR 東日本（東日本旅客鉄道）が開発し、現在６つ[24]の鉄道会社で導入されている共通乗車カード・電子マネーである。非接触 IC カードの通信規格であるサイバネ方式を使用している。名前の由来は「super urban intelligent card」の略で、スイっと通れるという意味も超えている。当初は自動券売機で乗車券を買わずに改札口を通過できるプリペイドカードのイオカードを置き換える目的で発売されたがが、今では定期券機能、グリーン券機能、駅構内や街なかのコンビニエンスストアや自販機の支払いに利用できる電子マネー機能が盛り込まれている。繰り返しの利用が可能なため、使用後の廃棄物が発生しないという利点がある。現在では、FeliCa や NFC 搭載のモバイル端末で利用できる「モバイル Suica」もある。交通会社系の電子マネーは多くの種類があり、相互利用が限定的であるのが何点であったが、2013 年 3 月 23 日から PASMO（関東の私鉄・バス）・Kitaca（北海道の JR）・TOICA（東海の JR）・manaca（名古屋の私鉄・バス）・ICOCA（関西の JR）・PiTaPa（関西の私鉄・バス）・SUGOCA（福岡の JR）・nimoca（福岡の私鉄・バス）・はやかけん（福岡市交通局）との乗車券機能の相互利用が可能になった。

[23] 通信工学と制御工学を融合し、生理学、機械工学、システム工学を統一的に扱うことを意図して作られた学問。
[24] 東日本旅客鉄道・伊豆急行・埼玉新都市交通・東京モノレール・東京臨海高速鉄道・JR バス関東

２－３－２－１－３．WAON（流通系電子マネー）

イオンリテールが発行する電子マネーである。SONY が開発した非接触 IC カードの通信規格 FeliCa を基に開発されている。IC カードタイプと FeliCa や NFC 搭載のモバイル端末で利用できるモバイルタイプがあり、IC カードタイプには他のカードとのジョイントカードが複数発行されている。名前の由来は「和音」、キャラクターの白い犬には「ハッピーワオン」という名前がある。2007 年のサービス開始と比較的遅いスタートであるが、2011 年で累計発行枚数 2770 万枚、利用可能店舗１５万店舗以上、年間利用金額は約 1 兆 26 億円と主要６電子マネーの中でトップである。流通系電子マネーの例として、他にセブン&アイホールディングス発行の「Nanaco」がある。

２－３－２－１－４．楽天 Edy（独立系電子マネー）

楽天 Edy 株式会社が提供する電子マネー。通信規格は FeliCa を使用し、それを搭載したカードや FeliCa または NFC を搭載した携帯電話やスマートフォンで利用できる。2,011 年時点での普及状況は、発行数が累計 6,420 万枚、利用可能店舗数 26 万店以上。クレジットカードや会員証、社員証[25]、学生証、キャッシュカードなど、多くの種類のカードに付加されている。また、2010 年まではゆうちょ銀橋や三菱東京 UFJ 銀行のクレジットカード機能付きキャッシュカードに付加されていたが、今ではその発行を終了している。

２－３－２－２．仮想マネー方式

仮想クーポンとしてコンピューターネットワーク間取引だけで利用する方式。特にサービス会社のインターネット上のサーバーと利用者のパソコンとの間で、ID/パスワードまたは秘密のパスワードにより管理された電子マネーをやり取りするものが主流である。オフライン方式の電子マネーの場合、その電子マネーを汎用性の高いものにするには小売店にまで行き届いたインフラの構築が必要となるが、仮想マネー方式の電子マネーはインターネット上の取引のみを対象としているため、インフラへの投資が比較的低くて済むというメリットが有る。また、シンプルなシステムであるために利用者の匿名性が高く情報漏えいなどのリスクが小さい。

２－３－２－２－１．Webmoney

KDDI の子会社である株式会社ウェブマネーが発行するプリペイド型仮想通貨。コンビニやゲームショップなどの端末を操作し、レジで現金を支払ってプリペイド番号を受け取る方法と直接レジカウンターで購入する方法がある。前者ではシート型、後者ではカード型の WebMoney が購入できる。ここに記載された英数字 16 桁の番号をインターネットサービスの支払い画面などに入力して決済する。当初の WebMoney は 1,000 ポイント・3,000 ポイント・5,000 ポイント・10,000 ポイントでしか購入できず、端数を支払った後の値段を利用するのが困難であった。しかしその後、残りの端数をためておけるウェブマネーウォレットのサービス開始や、900～10000 円まで 1 円単位で購入額を指定できる

25 ソニー、全日本空輸、三菱東京 UFJ 銀行、大和証券グループ、バンダイナムコゲームスなどで導入。

ジャストポイントなどのサービスが開始された。2011 年の決済額は 734 億円であった。また、近年のソーシャルゲームの台頭により、決済額は 2012 年に 1200 億円になった。

２－３－２－２－２．PASELI

コナミのアーケードゲーム機の対応機種でセーブデータなどを引き継ぐことのできた、e-AMUSEMENTPASS に付帯する形でスタートしたサービスである。名称の由来は「Pay Smart Enjoy Life.」の略である。100 円玉でプレイするより PASELI を利用したプレイのほうが安く、コナミ ID を設定した e-AMUSEMENT PASS に PASELI の設定をすることで利用できるようになる。PASELI のサービス開始は 2009 年であるが、2005 年に発売された初期型の e-AMUSEMENT　PASS でも利用できる。

２－３－３．ゲーム内通貨とリアルマネートレード

ゲーム機・PC の処理能力やインターネットの通信能力が向上した結果、多人数で同時に 1 つのサーバーに接続して RPG を楽しむことのできる大規模多人数同時参加型オンライン RPG（MMORPG[26]）が発売され、人気となった。世界には無数の MMORPG が存在するが、代表的なものとして「ファイナルファンタジー11[27]」等がある。これらの MMORPG の特徴として、「ゲーム内通貨[28]」がある。ゲーム内通貨とは、MMORPG の中における経済活動に使える通貨で、敵を倒す、物を売るなどの行為によって取得でき、それを利用してレアアイテム等を購入できる。また、プレイヤー同士でのアイテムの売買にも使用可能であり、MMORPG の中では擬似的な経済システムが成立している。つまり、ゲーム内という一定の制限内であれば、強制力を持つ立派な通貨として存在している。これらゲーム内通貨を現実の通貨で売買する行為を、リアルマネートレードという。リアルマネートレードはオンラインゲームの本掲示板でなくインターネット上の掲示板[29]で行われる。ほとんどのオンラインゲームではリアルマネートレードはゲームバランスを壊すなどの理由で利用規約違反に該当するが、それでもリアルマネートレードは後を絶たない。これらのゲーム内通貨は、発行主体がゲーム会社であり、本来現実の通貨としてはまったく価値がないが、リアルマネートレードを通し、間接的に現実通貨としての価値を持つことになった。

このリアルマネートレードを公認し、仮想世界内での経済活動を目的の中心としたサービスが、「セカンドライフ[30]」である。「メタバース[31]」と言われる仮想世界の中で、各自が物を作るな

---

[26] Massively Multiplayer Online Role Playing Game。

[27] スクウェア・エニックス社、2001 年サービス開始、有効会員数 55 万人。
http://www.playonline.com/ff11/index.shtml

[28] 前述のファイナルファンタジー11 のゲーム内通貨は「ギル」である

[29] RMT 掲示板　http://rmt.kakaran.jp/bbs

[30] 2003 年 4 月運営開始、運営は Linden Lab 社。利用者数はおよそ 100 万人

[31] Metaverse…コンピュータによって生み出され、インターネット上に存在する仮想世界。3 次元コンピュータグラフィクスによって 3 次元の立体空間として表現されるものが多い。MMORPG と違い、背景の物語、倒すべき敵などは存在せず、利用者上司の交流・商業活動や学術的な研究を主目的に活用されているものが多い。

どの経済活動を行う[32]。ゲーム内では「リンデンドル」という通貨により経済活動が行われているが、このリンデンドルはゲーム内の LindeX といわれる取引所で米ドルと交換できる[33]。米ドルとリンデンドルは常に変動するレートを形成しているため、リンデンドルは間接的にであるが、通貨としての価値をもつことになった。仮想世界上に存在し、リアルマネートレードによりいつでも望む分だけ現実の通貨に交換できるという考え方は、非常に魅力的であり、多くの人々をひきつけた。

２－３－４．暗号通貨の誕生

こうしてみてくると、ゲーム内通貨の思想を、仮想世界を通さずに、現実でやろうと考えたのが暗号通貨であると考えられる。ビットコイン決済機能のなかで、新しいとして注目されるようになった背景としてあげられるのが、その決済手数料の安さである。公開鍵暗号にせよ、ハッシュにせよ、ピアツーピアにせよ、技術自体が先進的というわけではない。それらを組み合わせることによって、低価格で、世界中を相手に決済できる仕組みが注目されているのである。グローバル化が進む中で、国境を越えて取引をする場合、決済にはいくつかの方法があるが、通常外国に現金を送金するには高額の手数料がかかる。また、現金や預金の送金は、原則としてドルを通じて行われるため、マイナーな通貨への送金となると送金手数料が非常に高額になる。比較的安いと言われるクレジットカードでも数百円の手数料がかかるため、数百円や数ドルと言ったような小額を決済する場合、決済する価格と手数料が同じ程度かかってしまい、決済手段として現実的ではない。しかしビットコインは、ビットコイン同士の取引であればほとんど無料で決済を行うことができる。これはサーバーを持たず、運用コストを各自で負担する P2P 方式の利点といえる。そのため、数百円を海外で決済するような場合に、ビットコインは非常に有用だといえる。ここに、ビットコインを新しい決済方法として迎える需要があると考えられる。

３－１．通貨の要件を満たしているか

ビットコインが通貨といえるかという問題は、経済学者の中で論争が続いている。が、ここでは単純に、先に述べた通貨の 3 要件を満たしているかを検討する。まず、決済機能である。ビットコインは現在、インターネット上の EC サイトや世界中で 1500 箇所以上の店舗で利用することができる。クレジットカードや電子マネーに比べると決して多い店舗数とは言えないが、限定的とはいえ、望む財と交換することができる。また、交換所を通して法定通貨に変換できるため、少なくとも「広義流動性がある」と認めることはできる。価値の尺度機能も、ビットコインと各国の法定通貨との交換レートがリアルタイムで公表されているため、モノやサービスの価格を換算してビットコイン表示にすることは容易に可能である。最後の勝ち保蔵機能についても、投機目的で、値上がりを期待してビットコインを保有している人が世界中にいるため、価値保蔵機能も認められていると言える。以上から、すべて限定された範囲とはいえ、ビットコインは通貨と言

[32] コンピュータによって生み出され、インターネット上に存在する仮想世界を「メタバース」という
[33] 2014 年 9 月現在、米ドルのみしか交換ができない。

える。しかし、政府の統計など[34]ではビットコインを通貨とみなしてはおらず、通貨でないとも言える。

３．マイクロペイメントサービスとしてのビットコイン

マイクロペイメントとは、少額決済を意味する言葉で、通常数百円や数ドルといったような少額の買い物を指す。数百円規模の決済は、日常生活上のカフェ、コンビニエンスストア、駅、飲食店などで日々膨大な量が発生しているが、マイクロペイメントといった場合には、現金を除いた、電子的な決済手段による取引の市場規模を指す。ビットコインは、このマイクロペイメント、特に国際的な取引におけるマイクロペイメントにおいて、その力を発揮すると考える。

３－１．マイクロペイメントとは

マイクロペイメントは、インターネット上でコンテンツ料金を集める方法として最近急激に進歩している。インターネット上での収益源は、広告収入が大きな柱であった。しかし、これを非常に多数のコンテンツ閲覧者に非常に少額の支払いを求めることで、利益を出そうとしたのがマイクロペイメントである。しかし通常、クレジットカードで支払うには数百円の決済手数料がかかり、決済手数料が購入対価を上回ってしまうことが多々ある。そのため、商取引としては現実的でなかった。

そこで、決済手数料を購入対価の数パーセントに抑えることで過度の負担をなくし、少額での電子決済を可能としたのがマイクロペイメントである。マイクロペイメントサービスで代表的なのは「Paypal」というサービスで、国内からの支払い受け取りに代金の 5%＋7 円、海外からの支払いの受け取りに 6%＋7 円という低コストの決済手数料を設定している。

マイクロペイメントが期待されるのは、雑貨などを扱う EC サイトなどがあるが、それより期待すべきなのは動画投稿サイトや絵の投稿サイトなどである。いわゆる「投げ銭」的な通貨として期待されている。今まではインターネット上で創造的なものを作った場合、その収益は広告に頼るしかなかった（いわゆる「振り込めない詐欺[35]」）。しかしマイクロペイメントサービスが台頭すれば、その商品の価値そのものに対価を払うことができるようになる。

３－２．マイクロペイメントサービスとしてのビットコイン

ビットコインの決済機能でもっとも注目すべきは、その決済手数料の安さである。取引所を経由したとしても、取引手数料は最大で 0.6%と、Paypal と比べても桁違いに安価である。この決済手数料の安さは、少額決済で小規模の事業を営む人に対し非常に魅力的である。また、インターネット上でコンテンツを配信し、その対価として少額の決済（いわゆる、おひねり・投げ銭）を

34 2014 年 3 月 6 日の政府見解は「ビットコインを通貨とは認めず、モノとみなす」というものであった。

35 ユーザーが自発的にお金を払いたくなるほど素晴らしい動画やツールを無償で公開した作者に対して敬意と感謝の気持ちを示すインターネット上の言葉。発祥は日本の「ニコニコ動画」という動画投稿サイトで、MikuMikuDance という 3DCG ムービーソフトウェアを無償で公開した作者である樋口 M 氏に対し「このように素晴らしいソフトが無料というのはあり得ない」「寄付させて」などのコメントが相次いたが、作者は寄付を含め一切の金銭の受け取りを断ったため、振り込め詐欺をもじって振り込めない詐欺と名付けられた。

要求するビジネスモデルを展開する際に、非常に有効な手段と言える。例として、Web 漫画を掲載し、その対価として 1 人当たり 250 円を得たとする。閲覧者（すべて国内からの支払いとする）が 5000 人いたとすると、その利益は表のようになる。

ビットコインでの取引の単位は、BTC で行われるが、今回は便宜上円とした。また、海外送金となると更に優位性は増していく。決済手数料のほかに、為替のリスクも考える必要があるからである。そして、Paypal は支払いと同時に、氏名とメールアドレスが相手に通知される[36]が、前述のようにビットコインは高い匿名性を持つため、上記のようなビジネスモデルに適していると言える。

項目	収入	手数料	収益
PayPal	250×5000＝125 万	（12.5＋7）×5000＝9 万 7500 円	115 万 2500 円
ビットコイン	250×5000＝125 万	1.5×5000＝7500 円	124 万 2500 円

４．クラウドファンディング用通貨としてのビットコイン

クラウドファンディングとは、不特定多数の人が通常インターネット経由で他の人々や組織に財源の提供や協力などを行うことを指す造語[37]であり、ソーシャルファンディングとも言う。ビットコインは、クラウドファンディングにおいてもその強みを発揮できると考える。

４－１．クラウドファンディングとは

クラウドファンディングは、クラウドソーシング[38]の考え方をもとにしている。すべてに共通するのは、プラットフォームを通じて多数の関係者を伴い、人々や組織がアイディアやプロジェクトを提案すると、それを支援する出資者が任意の金額を投資する。金額が目標の額に達したところで、人々はアイディアやプロジェクトを実行に移す。目標に達しない場合、投資した金額は出資者に戻ってくる。この方法により、資金調達のコストと資金繰りにかかわるリスクが大幅に下がるというメリットがある。投資に対する出資者の利益について、金銭的リターンのない「寄付型」、金銭リターンが伴う「投資型」、プロジェクトが提供する何らかの権利や物品を購入することで支援を行う「購入型」の 3 種類に大別される。クラウドファンディングは防災や市民ジャーナリズム、ファンによるアーティストの支援、政治運動、ベンチャー企業への出資 、映画、フリーソフトウェアの開発、発明品の開発、科学研究 、個人・事業会社・プロジェクトへの貸付など、幅広い分野への出資に活用されている。直接現金の融資を行うクラウドレンディング[39]も、クラウドファウンディングの一部として数えられることがある。クラウドファンディングは多くの関係者を伴うため、プラットフォーム[40]の作成と、国際的な投資、決済や税金に関する制度の制定や法律に

[36] Paypal でもビジネスアカウントに変更することで匿名化することは可能だが、手数料が割高になる。

[37] Crowd(群衆)＋funding(資金調達)

[38] 個人が多くの人々からわずかな寄与を集め、利用することで目標に到達する考え方。

[39] 融資を受けたい個人と融資をしたい個人をネット上で結びつける融資仲介サービス。クラウドファンディングは原則として融資に対する出資者の利益は現金によらないが、クラウドレンディングは現金を貸し、利子をつけて返すという点が異なる。なお、日本では貸金業法の規制があるため、海外と同じシステムでの業務は難しいとみられている。

[40] コンピュータにおいて、主に、オペレーティングシステム (OS) やハードウェアといった基礎部分を指す。本検討では、クラウドファンディングやクラウドレンディングなどに関係する人々を集めて、そこでのやり取りを可能とするシステム

関するルールの制定が重要な課題である。

４－２．クラウドファンディング用通貨としてのビットコイン

ビットコインはその手数料の安さという強みを生かして、クラウドファンディング用通貨としても台頭できると考えられる。実際、「BitcoinStarter」というサイトにおいて、プラットフォームが完成している。ビットコインによるクラウドファウンディングは、銀行口座を作れないような経済状態の人にとって、ビットコインによってのクラウドファウンディングは初期投資や導入のハードルという面で、大変に有利である。

５．ビットコインが抱える課題

５－１．技術上の課題

現状、ビットコインは強固な暗号化のもとに高い信頼性を保っており、それがビットコインの価値を決めているといえる。しかし、技術的な課題もある。たとえば、どんなに大量のビットコインを所有していたとしても、支払い用の暗号鍵を紛失すると永遠に使えなくなる。逆に、誤って秘密鍵を公開してしまった場合は、すべて盗まれてしまう。ペーパーウォレットとして保管しておく方法もあるが、このペーパーウォレットは紙幣というより「口座番号と暗証番号が記載された紙」であるため、保管には厳重な注意が必要である[41]。また、ビットコインのシステム自体は暗号化をしているが、取引所や交換所のシステムに攻撃をされてビットコインを失う可能性もある。次に、強固な暗号化とはいえど、ビットコインのシステム自体に攻撃できる脆弱性[42]があることである。攻撃方法には数多くあるため、以下に列挙する。

５－１－１．トランザクション展性を利用した「受け取ってない詐欺」

Mt.GOX の経営破綻問題で有名になった脆弱性である。ビットコインの取引データはデジタル署名されているため、改変があった場合署名の検証により検出される。しかし、取引データ全体に署名がかかっているわけでなく、一部、変更しても検出されない箇所がある。この部分を変えても取引自体の意味は変わらず、検証を通過してしまう。このような性質をトランザクション展性と言う。

一方、取引の識別子として取引データのハッシュ値を用いるが、ビットコインのネットワーク上の中継点の何処かでトランザクション展性を突いた改変が行われ、マイニングによりそちらが承認されると、送金者が取引データのハッシュ値を元に取引が承認されているか探そうとしてもブロックチェーンの中にその取引を見つけることができず、取引が承認されていることを確認できない。逆に受け手側は、手元の情報をブロックチェーンと同期させ自分のアドレス宛の入金を確認するため、取引が成功している事がわかる。

やサイトのことを指す。

41 テレビのキャスターが、ペーパーウォレットの例としてテレビに見せた結果、その QR コードを読まれて瞬時にビットコインを盗まれるという事件があった

42 コンピューターやソフトウェア、ネットワークなどが抱える保安上の弱点。正規の管理者や利用者など以外の第三者が保安上の脅威となる行為に利用できる可能性のある欠陥や仕様上の問題点。

ここで、受け手による入金されていないという虚偽の申請等によって、受け手には２回（トランザクション展性が続けて用いられた場合、数回)、同額の送金がされることになる。ただし、この問題は遅くとも 2011 年には指摘されていたことで、その辞典で送金皮の処理を行うソフトウェアを改修していれば問題は起きなかったと言われている。

５－１－２．シビル攻撃

ビットコインのネットワークに、自分が制御できるコンピュータを大量に参加させる。例えば他人のコンピュータをウイルスに感染させ、そこから参加させるようにすれば、インターネット上の異なる地点から P2P ネットワークに参加することになるため、より大きな影響を及ぼすことが可能になる。この攻撃は、さまざまな具体的な攻撃を行う前段階の攻撃となる。

５－１－３．エクリプス攻撃

取引データの中継を操作し、ビットコインのネットワークを分断する攻撃である。まず、P2P ネットワークの中で中継の要となる複数の地点に自分が制御できるコンピュータを配置する（これには、シビル攻撃を用いることもできる)。有効な配置ができたら、ネットワーク内にブロードキャストされている取引データやブロックが、一部、互いに届かないようにネットワークを分断する。分断されたそれぞれのネットワークでは、独自にブロックが作られて行き、結果としてブロックチェーンが分岐したまましばらく安定する。ブロックチェーンが分岐すると、分岐後は、それぞれの取引が起きたことになっている世界と起きていないことになっている世界が存在し、取引が起きていないことになっている世界でその取引に基づいた取引を試みると、承認されないということになる。それにより、ビットコイン全体の信頼性が失われることとなる。この攻撃は、ビットコインに対しての攻撃というより、ビットコインを構成する P2P に対する攻撃として、よく知られたものである。これ以外に、無意味なファイルの大量配布など、P2P に対する攻撃に対する知見の多くは、ビットコインにも適用できる可能性がある。

５－１－４．利己的マイニング

他のマイニングプールに参加しているコンピュータに無駄な計算をさせることで、自分のプールを相対的に有利にするという方法である[43]。利己的なマイニングを行うプールで、正しいブロックが得られても、それをネットワークにブロードキャストすることを遅延させ、他のプールからのブロップのブロードキャストを察知した時点で、自分が得た連続する１個以上のブロックをブロードキャストすることで、他のプールがマイニングしたブロックを無効化させることを試みる。ここで自分のブロックが有利に承認されるように、シビル攻撃により中継を操作することもできる。このことが少しでも成功すると、他のプールより有利に報酬を得られることにより、他のプールからマイナーが移ってくるようになる。これにより利己的マイニングが成功する可能性が更に高まり、新たなマイナーを呼ぶことにつながる。これを繰り返し、最終的にネットワーク全体の計算パワーの過半数を掌握できるというものである。

[43] 米国コーネル大学の研究者により指摘された。Ittay Eyal and Emin Gun　Sirer。Majority is not enough:Bitcoin mining is vulnerable 2013 より。

５－１－５．51%攻撃

マイニングに参加する計算パワーの過半数を掌握すると、ブロックチェーンをより長く伸縮させていくことができる。そのため任意の取引を承認させることができるという攻撃方法である。ビットコインの仕組みは「善意を持ったマシンが、51%以上存在すること」を前提として構築されているが、マイニングプールに計算パワーが集中してきた今、この攻撃が可能になることが現実味を帯びてきた。サトシ・ナカモトの論文では「この攻撃を実行に移せるだけのパワーを持っていたら、そのパワーを使って正規にマイニングをしたほうが得である」と言及されているが、これはあくまでビットコインが世界唯一の暗号通貨である場合を前提としており、他の暗号通貨の価値上昇のため、ビットコインを潰した方が利益になると判断した場合、この前提が崩れてしまう。ビットコインが社会インフラとして使われだした後、このような攻撃が行われることは、十分考えられる。

５－１－６．「世界」から切り離されたら

インターネットが世界に遍く広がっていると言える今でも、一部地域のインターネットが世界から分断される可能性は低くない。近年でも、エジプト革命[44]において、2011 年 1 月末から 2 月初めにかけ、1 週間エジプトのインターネットが遮断[45]された事例がある。また中国が「金盾（グレートファイヤウォール）」と呼ばれる、中国政府に都合の悪い情報をブロックするネット検閲システムがあることが知られている。また、アフリカなど通信インフラが整っていない国々では安定したインターネットへの接続そのものが不安定で、ビットコインがまともに使えない可能性は十分考えられる。つまり、ビットコインは結局はある国の政治的な安定に依存する。

５－２．制度上の課題

通貨（currency）には、「制度によって認められた貨幣」という意味が含まれる。ビットコインは、実態として限定的ではあるが通貨としての機能を有しているが、制度として「モノ」とされているという現状がある。脱税などの温床になるという懸念がある。直接決済はもちろんのこと、取引所を介した決済も社会的に保障されず、通貨としての信用は決して高いといえない。また、ロシアやインドなど使用自体を非合法化する国もある。

また、ビットコインをはじめとする暗号通貨は、その匿名性の高さから、犯罪などの資金洗浄に使われる可能性が高い。事実ビットコインは、麻薬や銃の売買を扱うことで名高いオンライン闇市場「シルクロード」での取引で用いられていたという事実がある。シルクロードは 2013 年 10 月に FBI により閉鎖されたが、その後、シルクロードは復活しており、他の闇市場の出現も後を絶たない。さらに、詐欺の横行も懸念される。取引所や交換所は、国から正当な資格を得てやっ

[44]エジプト革命（エジプトかくめい）は、エジプトの国内外において 2011 年 1 月より発生した大規模な反政府デモとそれに付随する事件の結果、ムバーラク大統領が辞任に至った革命。エジプト革命は、1952 年にエジプトが独立するための革命もあるため、「2011 年のエジプト革命」と区別することもある。

[45] 2011 年 1 月 27 日夜、エジプトのネットトラフィックのほとんどを占める 4 大 ISP（インターネット・サービス・プロバイダー）と携帯キャリアが、エジプト国内からのインターネットアクセスを遮断した。

ている銀行などと違い、ベンチャー企業がただやっているに過ぎないため、持ち逃げした場合、通貨としての保障を受けることが難しい。暗号通貨自体を詐欺目的で作り、ある程度の価値を持ったところで現金と換金し、その現金を持ち逃げするという詐欺が発生したこともあり、今後そのような問題は増加していくだろう。

５－３．発展上の課題

ビットコインが社会に浸透、インフラとして欠かせないものになるためには実店舗で使えることが必要不可欠である。2 章で見たように、ビットコインは取引が承認されるまで 10 分という時間がかかる。クレジットカードから見ると速いが、現金からすると遅い。決済をしてから 10 分間、承認を得ることができるまで店の中で待機してもらうと言うのは、一般的な買い物の場において現実的ではない。取引所を介することで即時取引が可能になるが、少額といえど手数料を支払う必要があり、これを誰が負担するかという問題が残る。アップルがビットコインの取引に関する純正アプリから撤退したという現状もあり[46]、全世界に遍く浸透するには相当の障害があると考えられる。

６．暗号通貨の多様化

ビットコインを支える技術や思想自体は公開されているものであり、複雑なものとは言えないため、ビットコイン以外にも、多くの暗号通貨が登場している。Crypto-Currency Market Capitalizations[47]によると、2015 年 1 月時点で 488 通貨が存在している。このなかから、特徴的なものを紹介する。

６－１．ビットコインから派生したもの

これらの暗号通貨は、本質的にはビットコインの特徴を受け継ぐためビットコインの脆弱性、制度的、発展的課題を引き継ぐが、ある点についてはビットコインの脆弱性を克服したものになっている。

６－１－１．LiteCoin（ライトコイン）

ライトコインは、ビットコインに次いで流通している通貨[48]である。後発であるため、開発者たちがビットコインについて問題と考えている部分について、いくつかの改善が施されている。具体的には①発行量の上限がビットコインよりも高く設定されていること、②マイニングの時間間隔をビットコインより短くしているため、決済の承認時間が短いこと、③マイニング専用ハードウェアの開発を難しくするため、メモリを大量に使うアルゴリズムが採用されていること、などが挙げられる。

６－１－２．DogeCoin(ドゲコイン)

ドゲコインは、ライトコインのソースコードを元に作られたデジタル通貨

46 ただし iOS デバイスでは、ブラウザからアクセスすることでビットコ
47 http://coinmarketcap.com/all/views/all/
48 2015 年 1 月現在の流通量は 5 億 2000 万ドルである。

である。柴犬がモチーフとなっている。ドゲコインには、発行量の上限が無く、マイニングにおける新規発行量も一定である。これらは、チップ用通貨としての特色が強い。

６－２．その他、特徴ある暗号通貨

６－２－１．NameCoin（ネームコイン）

ネームコインは、自らが DNS サーバー[49]の機能を持ち、ICANN[50]の影響下にない。ICANN は民間非営利団体であるものの、アメリカ商務省の傘下あり、インターネットガバナンスと呼ばれる国際問題となっている。そのため、自らが DNS サーバー機能を持つことは、「世界から切り離される」危険性を減らす。

６－２－２．Ripple（リップル）

Ripple Labs Inc が運営する暗号通貨。運営元が現金との交換を保証する[51]ことなどに、ビットコインとの違いがある。また、マイニングのためのマシンパワーを World Community Grid に使用し、癌などの研究に貢献できる。

７．ビットコインは通貨の未来をどのように変えるか

７－１．ビットコインは、世界共通通貨になることができるか

現在、対外取引の 90%は米ドルにて行われており、米ドルは基軸通貨（key currency）と呼ばれている。これにとって代わり、ビットコインが基軸通貨に、またその先の世界共通通貨になれるのかという疑問が浮かぶ。これは私見であるが、ビットコインが米ドルに代わる基軸通貨に、またその先の世界共通通貨になることは、きわめて難しいだろう。理由は 3 つある。前述したように、ビットコインは価値の保蔵機能が不安定である。今後落ち着いてくるとはいえ、中央銀行を持たないビットコインは、誰かが恣意的に価値を上下させることが不可能である。そのため、これだけ不安定なものを共通通貨にすることは難しいと思われる。次に、すでにビットコインを非合法だとした国があることである。数か国で非合法となっている通貨を世界の共通通貨にすることは容易ではない。最後に、ビットコインが世界通貨になるためにはその価値の絶対量が足りない。現在地球上にあるビットコインの流通額は、世界でおよそ 1 兆円規模とされている。円の流通量が現金ベースで 81 兆 4215 円と考えると、1 兆円という数字は非常に微々たるものであることがわかる。

---

[49] ドメインネームシステムを担う、コンピュータやサーバーソフトウェアのこと。ホストの識別子を利用者が理解しやすい形式とコンピュータがインターネットプロコトルで通信するために必要な識別情報を対応付ける仕組み。

[50] Internet Corporation for Assigned Names And Numbers　インターネットの IP アドレスやドメイン名などの各資源を全世界的に調整・管理することを目的とし、1998 年に設立された民間法人。

[51] グリッド・コンピューティング技術を用いて、世界中のパソコンから集めた処理能力を結集することで　、仮想的なスーパーコンピュータを作り出し、それを基盤として社会的に意義の高い研究活動に世界最大規模の演算能力を提供する人道的活動。エイズを始めとする未知のウイルスや病原体への対応、新薬の開発（バーチャル・スクリーニング）につなげたり、病気の処置法の探求など、生体工学分野を中心に人類の脅威とされる課題の克服に貢献するため、ボランティア・コンピューティングとも言われる。

７－２．通貨と決済サービスの未来

では、ビットコインはどのような場面で通貨としての価値を見出されるのか。それは、前述のとおり、マイクロペイメント、特に国際間でのマイクロペイメントサービスとクラウドファンディング用の通貨として期待を寄せられているという部分である。コストが非常に低く、匿名性が高いというビットコインは少額を国際的に決済する場合、威力を発揮する。

おわりに

Ｐ２Ｐ（ピアツーピア）という方法により決済を完了し、他の法定通貨を価値の後ろ盾としない「暗号通貨」が台頭してきている。本研究では、最も取引量の多いビットコインを例に挙げ検討を行った。暗号通貨は決済サービスの多様化と国家通貨への不信の中で、リアルマネートレードができるゲーム用通貨を暗号学的に基づく電子的支払いシステムにより、通貨としての価値を持たせ、流通させることを想定して誕生した。特徴はその決済手数料の安さで、特に国際間の小額決済について威力を発揮すると考えられる。

次に「通貨制度」と「情報技術」という 2 つの面からビットコインをはじめとする暗号通貨が「通貨」として確立されているのかを検討した。ビットコインは P2P と暗号化技術により支えられており、理論としては非常にシンプルなのでコストを抑えながら運用できるという特徴がある。

最後にそれらが一時のバブルとして終わることなく、今後ひとつの価値を認められた通貨として世界に通用するためには技術上、制度上の課題があり、技術上の課題は構造的な脆弱性を含むものであることがわかった。これらにより、ビットコインは今後社会のインフラとして浸透し、世界の基軸通貨となれるようなものではなく、マイクロペイメントやクラウドファンディングなど、一部の人々が便利さを享受するものにとどまると考えた。ただ、国際的な通貨への不安は今日でも尽きること無く、現在も貨幣は品行、格差、自然と生活の破壊など様々な問題を生んでいる。多様な暗号通貨が互いに互いの脆弱性を補完しあうことにより、現在指摘されている構造上の脆弱性を克服し、国際基軸通貨となりうるような暗号通貨が登場すると、世界の経済社会は、これから変わっていけるかもしれないと考える。

参考文献

ニューズウィーク日本版 2014 年 2 月 25 日「新通貨ビットコインの正体」阪急コミュニケーションズ社
『暗号が通貨になる「ビットコイン」のからくり』吉本佳生・西田宗千佳　講談社
『日本の効果流通量の構造変化』財務総合政策研究所
『これで分かったビットコイン：生き残る通貨の条件』佐藤賢爾 次郎太郎社エディタス
『貨幣という謎-金(きん)と日銀券とビットコイン-』西部忠　NHK 出版新書
『日本の税金 新版』三木義一　岩波新書
『ソーシャルファイナンス革命～世界を変えるお金の集め方～』慎 泰俊　生きる技術！業書