仮想通貨の現状と将来性
～ビットコインを中心に～

中島真志

はじめに

皆さん、こんにちは。ただいま御紹介いただきました麗澤大学の中島です。今日は「仮想通貨の現状と将来性～ビットコインを中心に～」というテーマでお話しします。

まず簡単に自己紹介いたします。もともと長く日本銀行におりまして、調査統計局、金融研究所、国際局、金融機構局などに勤務した他、ＢＩＳ（国際決済銀行）に出向して仕事をしたことも

あります。二〇〇六年から麗澤大学に移りまして、研究活動を行っております。日銀時代から、主に資金決済や証券決済の分野に従事してきたこともあり、『決済システムのすべて』や『証券決済システムのすべて』といった本を書いています。

ビットコインは、世界中に自由にお金が送れるツールとして、突然、決済のフィールドに入ってきました。自分のエリアに飛んできた球は拾わざるを得ません。そのようなこともあって、徐々にこの世界に入っていくことになりました。二〇一

七年一〇月に『アフター・ビットコイン』を上梓しました。ちょうどビットコインがブームになっていたこともあり、大手の書店でベストセラーになりました。

この本には、幾つかの特徴があります。一つ目は、ビットコインの仕組みが比較的わかりやすく書いてあることです。二つ目は、ビットコインについて批判的に検討していることです。三つ目は、ビットコインにとどまらず、それを支える技術であるブロックチェーンを詳しく取り上げ、これが今後の本命になると書いていることです。おかげさまで、発行部数は五万部まで来ており、韓国語の翻訳も出ています。

今日は、そもそもビットコインとは何か、ビットコインを支えている仕組みは何か、ビットコインは夢の通貨なのか、悪魔の通貨なのか、さらには、将来に向けてビットコインをどのように見ていけばよいのかといった点についてお話をさせていただきます。

一、そもそもビットコインとは何か？

（ビットコインの始まり）

そもそもビットコインとは何でしょうか。二〇〇八年にサトシ・ナカモトという人物が論文を発表しました。その論文を基に、二〇〇九年一月に初めてのビットコインが発行されました。この一月で発行開始後一〇年が経ちました。サトシ・ナカモトは、名前だけ見ますと日本人のようですが、実際には日本人ではないのではないかと言われています。

日本では、ビットコインは仮想通貨（バーチャル・カレンシー）と呼ばれてきました。これは、

インターネットを通じて取引が行われ、紙幣やコインのように目に見える形がないためです。他方、海外では、一般に暗号通貨（クリプト・カレンシー）と呼ばれています。ビットコインが高度な暗号技術を使っていることを踏まえたものです。

（ビットコインの特徴）

ビットコインの特徴の一つは、中央に管理者がいないことです。プログラムが通貨の発行を制御しており、中央の管理者によるガバナンスは行われていません。

二つ目は、独自の通貨単位を持っていることです。ビットコインの通貨単位はＢＴＣです。このため、円やドルとの間で交換レートが発生し、それが上がったり下がったりします。〇・一ＢＴＣ、〇・〇五ＢＴＣなど、小数点以下の取引も可能になっています。最小の単位は〇・〇〇〇〇〇〇一ＢＴＣ（小数第八位）であり、サトシ・ナカモトにちなんで一サトシと呼ばれています。

三つ目は、私のような中央銀行出身者にとって不思議に感じられる点ですが、発行主体が存在しないことです。銀行券は中央銀行の負債として発行されますが、ビットコインの場合は、誰の負債でもありません。

四つ目は、プルーフ・オブ・ワークとマイニングです。難しい計算をすることによって安全性が確保され、その計算ができた人にリワード（報酬）が与えられる仕組みになっています。

五つ目は、取引の確定までに時間がかかることです。一つのブロックを作るのに、概ね一〇分かかります。

六つ目は、発行上限が設けられていることです。二一〇〇万ＢＴＣという上限があらかじめ決

まっています。通貨は、発行量が多くなりますとインフレになり、価値が下落します。サトシ・ナカモトは、これを嫌ったのではないかと言われています。

二、ビットコインを支える不思議な仕組みとは？

（ビットコインの受け払いに必要なもの）

次に、ビットコインの仕組みについて簡単に御説明します。

まず、ビットコインの受け払いに必要なものとして、ウォレットとビットコイン・アドレスがあります。ウォレットは電子的な財布であり、パソコンやスマホの中にデジタル・ウォレットが作られ、そこにビットコインの残高情報が収められます。ビットコイン・アドレスは口座番号のようなもので、約三〇桁の英数字から成る文字列です。相手のアドレスを指定してビットコインを送付します。

一つのウォレットに対して、複数のアドレスを作ることができます。インターネットを通じて、あるアドレスから他のアドレスにビットコインが送られますと、どのアドレスからどのアドレス宛てに、何月何日何時何分に幾ら送られたのかが、全て、インターネット上で公開される仕組みになっています。非常に透明性が高い仕組みのように見えますが、わかるのは、例えば、アドレスＡからアドレスＤに、何月何日何時何分に幾ら送られたかということだけです。アドレスＡが誰のアドレスで、アドレスＤが誰のアドレスなのかはわかりません。ビットコインには高い匿名性があると言えます。これをメリットと考える人もいますが、いろいろな問題が起きているのも事実です。

（ビットコインを入手する三つの方法）

ビットコインを入手するためには三つの方法があります。

一つ目は、仮想通貨取引所（日本では「仮想通貨交換業者」と呼ばれます）で口座を作り、円との交換でビットコインを購入することです。日本には、今、ビットフライヤーやコインチェックなど、金融庁の登録業者が一七社あります。これらの業者で口座を作りますと、簡単にビットコインを購入することができます。

二つ目は、商品やサービスの対価としてビットコインを受け取ることです。ビックカメラやエイチ・アイ・エスなど、ビットコインで支払いができることをウリにしている業者があります。

三つ目は、ビットコインを採掘することです。複雑な計算処理を行って、その対価としてビットコインを受け取るものです。詳しくは後でお話しします。

（Ｐ２Ｐ型ネットワーク）

ビットコインの大きな特徴は、Ｐ２Ｐ型のネットワークを採用していることです。このことが理解できないとビットコインの革新性はわかりません。

従来は、クライアントサーバー型ネットワークが主流でした。中央に大きなサーバーがあり、そのサーバーとクライアントが通信を行って、さまざまな情報が処理されます。

他方、ビットコインの場合、個々のコンピューター（ノード）が、互いに対等の立場で直接通信を行うという、フラットな分散型のモデルが採用されています。どこにも中央がなく、全てのコンピューターが同じデータを持ち合い、どこかで取引が行われると、全てのコンピューターがデータ

ベースを書き換えるという仕組みになっています。ここが革新的な点です。

（ビットコインを支えるメカニズム―ブロックチェーン）

ビットコインの安全性を確保する仕組みがブロックチェーンです。これは、取引データを入れたブロックを、時系列的にチェーン状につなげて記録していく仕組みのことです。ブロックの一つ一つが帳簿に当たります。この帳簿を一〇分に一回ずつ作って取引を確定させていくことになります。いったんブロックに入りますと、データを変更することはほぼできません。このため、コインの偽造や二重使用ができないという仕組みになっています。

ブロックチェーンを使って取引をする仕組みを御説明します。

まず、AさんからBさんにビットコインを送るという取引をネットワークに送ります。インターネット上にはトランザクション・プールという待機場所があります。ブロックを作る人は、そこから取引データをまとめて自分のブロックに持ってきます。そのとき、二重使用や残高不足がないかどうかを確認します。そして、そのブロックに対して難しい計算をし、計算結果をブロードキャストします。ネットワーク上で、さまざまな人が、その計算が合っているかどうか検算を行います。検算は容易にできますので、計算が合っていることが確認されれば、その計算結果が承認されます。そうしますと、新しいブロックができ、それがこれまでのブロックの後に追加されます。これによって、AさんからBさんへのビットコインの送金が無事完了することになります。

技術的な話になりますが、ブロックには三種類

のデータが入っています。一つ目は取引のデータで、ブロックを作る人がトランザクション・プールからまとめて持ってきたものです。二つ目が前ブロックのハッシュ値、三つ目がナンス値です。

ハッシュ値は、膨大なデータを圧縮関数のハッシュ関数に入れて算出されます。六四桁など一定の長さに圧縮された英数字から成っています。元のデータが少しでも異なると、全く異なったハッシュ値が出てきます。さらに、計算してみないと、どのようなハッシュ値が出てくるかもわかりません。

（プルーフ・オブ・ワーク）

もう一つのキーワードはプルーフ・オブ・ワークです。端的に申しますと、ナンス値を計算することです。ナンス値を計算するに当たっては、ハッシュ値の先頭に一定の数以上のゼロが並ぶようにしなければなりません。

先ほども申しましたように、ブロックには三種類のデータが入っています。一つ目の取引データは、トランザクション・プールからまとめて持ってきたものなので動かせません。前ブロックのハッシュ値も、既に決まっておりますので動かせません。このため、動かすことができるのはナンス値だけということになります。これをいろいろと動かして、先頭に一定の数以上のゼロが並ぶような、現ブロックのハッシュ値を計算するわけです。これが、プルーフ・オブ・ワークです。

これは、実は相当難しいことです。総当たり法で、ナンス値にいろいろな数字を入れて、ハッシュ値を計算してみるしかありません。ナンス値は、一桁かもしれないし、一〇桁かもしれないし、あるいは一〇〇〇桁ないし一万桁かもしません。ともかく、ハッシュ値の先頭に〇〇〇〇……

が並ぶものを探し出し、それをネットワークにブロードキャストするわけです。

（マイニング）

このような難しい計算を行って、世界で最初に適切な答えを求めることができた人に、報酬（リワード）として新しいビットコインが発行されます。新たなコインが発行されるのはこのときだけであり、これが唯一のコインサプライの方法ということになります。ビットコインの場合は、最初の人が報酬を総取りするという方式になっています。

これは、計算によって無から有を作り出すことに他ならず、鉱山で金を探し当てるのと同じですので、マイニング（採掘）と呼ばれます。また、そのような計算をする人はマイナー（採掘者）と呼ばれます。マイニングは、ビットコインの取引を承認する仕組みであり、ビットコインの安全性を確保するためにはどうしても必要な作業です。二四時間三六五日、誰かがこのような難しい計算をするようにしなければなりませんので、経済的なインセンティブとしてリワードが与えられることになっています。

（ハッシュ値によるブロックの連続性）

現ブロックは、取引データ・ナンス値・前ブロックのハッシュ値から成っています。先ほど申し上げた手続きで得られた現ブロックのハッシュ値を次のブロックに入れます。次のブロックでは、このハッシュ値と新たに持ってきた取引データを基に、次のブロックのナンス値とハッシュ値が算出されます。そして、ここで得られた次のブロックのナンス値を、さらにその次のブロックに入れることによって、次々にブロックが連続して

いく仕組みになっています。一部でも取引データが変りますと、ナンス値が変わり、ハッシュ値も変ってしまいますので、連続するブロックの全体を計算し直さなければならなくなります。このため、取引データを変えることが極めて困難な仕組みになっているわけです。

三、ビットコインは、夢の通貨か、悪魔の通貨か？

(1) ビットコインへの二つの見方

ビットコインに関しては、大きく二つの見方があります。

一つは夢の通貨だというものです。日本のマスコミは、「通貨の未来を変えるもの」「通貨の革命」「素晴らしい」という論調で取り上げてきたように思います。これを受けて、日本ではビットコインブームが起きました。二〇一七年から二〇一八年の初め頃にかけて、日本の取引シェアは全世界の約三〇％から四〇％を占めました。日本人だけがはしゃいでいたように思います。

他方、悪魔の通貨だという見方もあります。欧米の銀行関係者は、ビットコインを指してevilあるいはviciousと言います。このような邪悪なものは金融取引には使えないというわけです。彼らはビットコインという言葉を使いたがりません。口にするのも汚らわしいという感じです。このため、ビットコインは規制すべきとなり、例えばグーグルやフェイスブックなどでは、仮想通貨に関する広告は一切掲載されていません。また、クレジットカード会社も、クレジットカードで仮想通貨を買うことはできないようにしています。

(2)　時々、盗まれたり、なくなったりする（盗難・流出事件）

ビットコインの問題点の一つ目に挙げられるのは、時々、盗まれたり、なくなったりすることです。

有名なのはマウント・ゴックス事件です。二〇一四年、ビットコイン取引所のマウント・ゴックスが突然取引を中止し、その後すぐに破綻しました。同社は、当時、世界最大手の取引所で、世界の取引量の七割のシェアを占めていました。同社は、当初、外部からのハッキングでビットコインがなくなったと説明していました。しかし、後日、フランス人の社長が横領していたことが明らかになりました。このときは、取引所の管理が甘かっただけで、ビットコインに罪はないという、ビットコイン擁護派の見方が強かったように思います。

しかし、盗難・流出事件はこれだけでは終わりませんでした（図表1）。二〇一六年には、香港のビットフィネックス、二〇一七年には、韓国のユービット、二〇一八年には、日本のコインチェックで盗難・流出事件が起こりました。コインチェックの場合、盗難・流出額は五八〇億円という巨額に上りました。その後も、韓国、イスラエル、日本、ニュージーランドなどで同様の事件が起きています。二ヶ月に一回の割合で、世界のどこかで盗難・流出事件が起きていることになります。

この一〇年間、ビットコイン自体の仕組みが破られたことはありません。しかし、ビットコインの保管や流通も含めたシステム全体には問題があるように思います。銀行や証券会社に預けた預金や証券が盗まれたり、なくなったりするようでは、安心して預けることはできませんが、仮想通

図表１　仮想通貨取引所からの盗難・流出事件

実は他にもある盗難・流出事件
－仮想通貨取引所は、けっこう頻繁に「GOXする」－

発生時期	取引所	所在国	流出した仮想通貨	被害額	事件後
2016年8月	ビットフィネックス	香港	ビットコイン	75億円	補償
2017年12月	ユービット	韓国	ビットコイン	60億円	破産
2018年1月	コインチェック	日本	NEM（ネム）	580億円	補償
2018年2月	ビットグレイル	イタリア	NANO（ナノ）	200億円	破産
2018年6月	コインレイル	韓国	Pundi Xなど	44億円	再開
2018年6月	ビッサム	韓国	ビットコインなど	19億円	補償
2018年7月	パンコール	イスラエル	イーサなど	20億円	取引所分のみ
2018年9月	Zaif（テックビューロ―）	日本	ビットコイン、モナコインなど	70億円	補償
2019年1月	クリプトピア	NZ	イーサなど	18億円	n.a.

・保管や流通も含めたシステム全体の安全性には、やや問題？

貨の世界では、しばしばそのような事件が起きているのが実情です。

（問題の背景―コインチェックの場合）

先に言及したコインチェックは、当時、まだ正式に登録しておらず、みなし業者として営業を行っていました。同社の管理体制には幾つもの問題がありました。

一つ目は、ホットウォレット、つまり、ウォレットをインターネットにつなぎっ放しの状態で、ビットコインを管理していたことです。通常、多額のコインを保管する場合は、コールドウォレットと言いまして、ウォレットをインターネットから遮断した状態で管理します。外部からアクセスされるのを防ぐためです。

二つ目は、マルチシグ（複数の鍵）を使わず、一つの鍵で管理していたことです。複数の鍵があ

れば保護することが可能であったと思われますが、一つの鍵で管理していたため、その鍵が破られたことで、ウォレットの中のものが全て盗まれてしまうことになりました。

三つ目は、五八〇億円という巨額のコインをたった一つのウォレットで管理していたことです。これが最大の問題であったと言えましょう。仮想通貨の世界では、個人でも、金額が大きくなってきたらウォレットを分けることが推奨されています。にもかかわらず、業者が、五八〇億円ものビットコインを一つのウォレットに入れていたわけです。ずさんとしか言いようがありません。

（問題の背景―テックビューロの場合）

もう一つ、テックビューロの事件を取り上げます。同社は登録業者であり、金融庁が登録を認めた業者において盗難・流出事件が起きたという意味では、コインチェック事件より問題は深刻ではないかと思いますが、マスコミはあまり騒ぎませんでした。

この事件の問題点は、またしてもホットウォレットで管理していたことです。もう一つ、金曜日に不正アクセスがなされたにもかかわらず、発覚したのが月曜日に社員が出勤してきてからで、事件に気づくのが遅過ぎるのではないかという指摘もなされました。

さらに、コインチェックの事件後、金融庁が同社に検査に入り、二回にわたって業務改善命令が出されていました。当然、ホットウォレットについても指摘がなされていたはずですが、それを放置したままになっていました。金融庁から業務改善命令を受けたにもかかわらず、それを無視して何も対応しないということは、金融機関の場合は

ありえないことです。どうやら、同社は、金融機関のカルチャーではなく、ＩＴ企業やベンチャー企業のカルチャーで運営されていたようです。

(3) 犯罪に使われる（シルクロード事件）

ビットコインの問題点の二つ目は、犯罪に使われることです。

最も有名なのはシルクロード事件です。シルクロードは違法な薬物などを販売していた闇サイトで、そこではビットコインが決済手段として使われていました。インターネットで買い物をする場合、通常であれば銀行振り込みやクレジットカード決済が使われます。しかし、違法薬物を売買する際に、そのような方法で決済すれば一発で足がついてしまいます。そこで、ビットコインの高い匿名性が悪用されたわけです。このサイトは二〇一一年に作られ、二〇一三年に運営者がＦＢＩに逮捕されました。この間の売り上げは、一二億ドル（約一二〇〇億円）と驚くべき金額に上っています。

この事件によって、ビットコインは違法取引に使われるものだというダーティーなイメージが付いてしまいました。それとともに、世界中の人が、違法薬物の取引にはビットコインを使えばよいことに気づいてしまいました。シルクロードは閉鎖されましたが、その後も、ハンザ、アルファベイ、ドリームマーケットなど同じようなサイトが次々に出てきました。一つを閉鎖しても、また次のものが出てくるという形で、イタチごっこが続いています。

実際のシルクロードの画面を見ますと、マリファナ、ＬＳＤ、ヘロインなど、口に出すのも汚らわしいような物がいっぱい売られています。価

格は、ビットコイン建てで表示されており、ビットコインをシルクロードに送りますと、そうした違法薬物が送られてくるわけです。こうした形でビットコインが使われたことで、欧米の金融機関の人がビットコインを邪悪なものだと感じてしまうことになりました。

実は、日本でも同じようなことが起きています。二〇一七年一一月の新聞に、「危険ドラッグのネット販売　仮想通貨で決済　摘発逃れか」という記事が掲載されました。これによりますと、危険ドラッグをインターネットで販売するに当たって、対価をビットコインで支払わせていたようで、まさにシルクロードのやり方をそのまま真似たものになっています。これまでは、麻薬取引の決済は現金で行うしかありませんでしたが、今や、ビットコインを使うことで、インターネット上で取引が完結するわけですから、犯罪者にとってこれほど便利なものはないと言えましょう。

（ランサムウェア）

犯罪に使われているもう一つの例として、ランサム（身代金）ウェアでの利用があります。二〇一七年五月、一五〇ヶ国でランサムウェアのウイルスがばらまかれました。これに感染しますと、パソコンが動かなくなり、「あなたのコンピューターは乗っ取られました、ファイルは回復できますが、そのためには三〇〇ドル相当の身代金をビットコインで支払う必要があります」という画面が表示されます。画面の下の方には、犯人のアドレスも堂々と書かれています。銀行の口座番号をこのようなところに書くことはできませんが、ビットコインのアドレスであれば誰のものかわかりませんので、このようなことができるわけです。身代金の受け渡しに使うには非常に便利で

す。

このランサムウェアでは言語が選択できるようになっています。日本語の他に、英語、ドイツ語、フランス語、ロシア語、中国語など二十数カ国語で表示されるようになっており、非常に顧客に優しい作りになっています。これは、画面の表示を読んでもらえないと脅迫にならないためです。

画面の左側には二つのカウントダウンタイマーが表示されています。上のタイマーは、そこに表示された時間内に支払わないと、身代金が倍になることを示しています。下のタイマーは、そこに表示された時間内に支払わないと、完全にデータが消去されることを示しています。三〇〇ドル相当（約三万円）の身代金で、全てのデータが復元できるのであれば安いものだと考えて、身代金を支払った人が世界中にかなりいたのではないかと思われ、よいビジネスになったのではないでしょうか。

ビットコインの出現によって、ランサムウェア業界は、毎年、倍々ゲームで伸びていると言われています。

（匿名性が高い）

最近の研究によりますと、ビットコイン利用者の四分の一が違法ユーザーで、取引量の四四％が違法な取引に使われているとのことです。先ほども申しましたように、アドレスは全てわかっておりますので、例えばシルクロードと取引を行っていたアドレスは、違法な取引をしている人間のものであることがわかります。そこから芋づる式に辿っていきますと、ビットコインの利用者の四分の一が違法ユーザーであることがわかったということです。

（ビットコイン・ネットワークと取引所の関係）

ビットコインの取引には、オン・チェーンとオフ・チェーンの二種類があります。

オン・チェーンの取引は、サトシ・ナカモトが考えていたような分散型で、各ノードが自分でウォレットを作り、秘密鍵を管理するものです。

他方、オフ・チェーンの取引は、サトシ・ナカモトが大嫌いな中央集権型で、仮想通貨取引所がウォレットを持ち、秘密鍵を管理しています。その取引所に口座を持っている人たちは、ウォレットや秘密鍵を持っておらず、仮想通貨取引所にアクセスし、パスワードを打ち込むことによって自分の口座を見ているわけです。オン・チェーンの取引は素人には難易度が高いため、オフ・チェーン、つまり、ネットワークから外れたところで、ビットコインの取引を行っているわけです。ダブルカウントが多少あるかもしれませんが、日本では、約三六〇万人が仮想通貨取引所に口座を持って取引をしています。

なお、先ほど、ビットコインの利用者の四人に一人が違法ユーザーだと申しましたが、これはオン・チェーンで取引をしている人を念頭に置いたもので、オフ・チェーンでビットコインを取引している人とは区別する必要があります。

(4)　規制の抜け穴に使われる

（世界の九割以上を中国が爆買い）

ビットコインの問題点の三つ目は、規制の抜け穴に使われるということです。

二〇一七年夏までの一年間について、世界のビットコイン取引の取引所別シェアを見ますと、ＯＫコイン、フオビ、ＢＴＣチャイナという三つの中国の取引所が九三％を占めています。通貨別の取引シェアを見ても、元が九四％を占めていま

す。ここから、世界のビットコインの九割以上を中国人が爆買いしていたことがわかります。ビットコインは生まれて間がなく、主に欧米で売買されているというイメージがあるかもしれませんが、実際は、中国人が大部分を買っていたことになります。

それでは、なぜこれほど中国人がビットコインを爆買いしていたのでしょうか。二〇一五年に人民元の切り下げがあり、人民元の先安感が出ました。大量の人民元を持っている中国の金持ちは、このまま人民元を持ち続けると目減りすると考え、人民元をドルに換える動きに出ました。それに対し、当局は、元々厳しかった資本流出規制をさらに厳しくしました。このとき、金持ちが目をつけたのがビットコインです。ビットコインは資本流出規制の対象になっておりませんでしたので、まさに規制の抜け穴としてとりあえずビットコインに換えておこうという動きが起きました。さすがに中国当局もこれに気がつきました。二〇一七年の春頃から立入検査が行われ、秋には先ほどの三つの取引所が強制的に閉鎖されました。悪質な例が多く見つかったのだと思います。

（誰がビットコインを採掘しているのか）

ここで、マイニングがどのように行われているのかを見てみます。ビットコインが生まれた頃、マイニングは、サトシ・ナカモトが世界でただ一人行っていたようです。その後、マイニングの難易度が上がってきたため、最近では、大規模なマイニング・ファームが専用のコンピューターをズラッと並べてマイニングを行うようになりました。

マイニング・ファーム毎のシェアを見ますと、中国の一〇社が世界の七割を占めています。さら

に、これを含む一三社が世界の八割を占めており、寡占化が進んでいる状況です。マイニングのためには、大量のコンピューターを二四時間三六五日稼働させておく必要があります。このため、日本をはじめ電気代が高い先進国では、マイニングを行っても全くペイしません。中国のマイニング・ファームが高いシェアを占めているのは、中国の電気代が安いためです。

こうしてお話ししている間にも、一〇分に一回ずつビットコインの新しいブロックができており、その度にリワードが支払われています。今、リワードは一二・五ＢＴＣで、一ＢＴＣは約四〇万円ですから、約五〇〇万円に相当するビットコインが一〇分に一回の割合で新しく発行されていることになります。そして、そのうちの七割は中国のマイニング・ファームに支払われているわけです。

（中国のマイニング・ファーム）

中国のマイニング・ファームの実情を御紹介します。

四川省のカンゼ・チベット族自治州にあるマイニング・ファームでは、山間部の発電所のすぐ脇に採掘工場が設置され、できたての電気でマイニングを行っています。採掘工場には、専用のコンピューターが並べられ二四時間三六五日マイニングを行っています。

世界最大手のビットメイン社のマイニング・ファームは、内モンゴル自治区にあります。細長い、巨大な体育館のような採掘工場が、全部で七棟並んでいます。大変なボリュームです。採掘工場の中に入りますと、向こうが見えないぐらいの奥行きがあります。マイニング専用のコンピューターが手前から奥までずらっと並んでいます。

先ほども申しましたように、世界中で第一位に

ならないとリワードは与えられません。要するに、同社を上回るような投資をしないと、マイニング競争に勝てないということです。最近、日本企業でマイニングに参入すると言っているところがありますが、人ごとながら心配になってしまいます。

(5) 取引量に限界がある

ビットコインの問題点の四つ目は、取引量に限界があることです。

ビットコインでは、一〇分に一回ずつブロックが作られます。そして、そのサイズは、安全性の観点から最大一メガバイトと決められています。要するに、一〇分間の取引を全て足し合わせたものが、一メガバイトに収まらなければならないということです。逆算しますと、全世界の一秒間の取引件数は七件が限界ということになります。非常に非力なシステムと言わざるをえません。

比較のために申しますと、ＶＩＳＡのネットワークでは、全世界で一秒間に五万六〇〇〇件の取引ができるようです。これと対比しますと、一秒間に七件というビットコインのネットワークはおもちゃのようなものに見えてしまいます。サトシ・ナカモトは、実験のために今のようなビットコインを作ったのではないでしょうか。

一秒間に七件しか取引できない通貨が、果たして世界を変えるような通貨になれるのでしょうか。世界中のモノやサービスの取引の決済をしようとしますと、基本的なところで限界があると言わざるをえません。ビットコイン推進派は、わかっていてもこのことを言いませんが、致命的なことと言わざるをえないように思います。

(6)　電力を浪費している

ビットコインの問題点の五つ目は、大量の電力を浪費していることです。

マイニングのためには、大量のコンピューターを二四時間三六五日回し続けなければなりませんので、大量の電力を消費します。マイニングのための電力消費は、今、国としてカウントしますと世界で五三番目に相当します。具体的には、ペルー、香港、イラク、「ビットコイン」、シンガポール、ポルトガル、ウズベキスタンという順番になっています。スイス、デンマーク、チェコなどの中規模の国をしのぐ消費量です。アイスランドでは、一般国民が使っている電力より、マイニング用の電力の方が多くなっています。

海外の事例ですと、あまり実感が湧かないかもしれませんが、ビットコインのマイニングのための電力使用量は、東京都の全電力使用量を上回っています。一三〇〇万人が暮らしている東京の電力使用量より、ビットコインのマイニングのために使っている電力の方が多いのは、異常事態ではないでしょうか。

中国では石炭火力による発電が最も多いので、石炭を燃やしてビットコインのマイニングをやっていることになります。したがいまして、ビットコインは、地球環境にも深刻な影響を及ぼしていると言えます。しかも、多量の電力を使って計算しているのは、ナンス値という使い捨ての何の役にも立たないものです。そのようなもののために、これほど膨大な電力を消費してもよいのか甚だ疑問と言わざるをえません。

(7)　ビットコインの背景にある思想とは？

サトシ・ナカモトはなぜこのようなものを作ったのでしょうか。

彼の最初の論文を読みますと、「信頼関係のない者同士で価値をやりとりできる仕組み（trustless payment system）を作りたかった」と書かれています。例えばAさんがBさんにお金を送る場合、通常は自分の銀行から相手の銀行にお金を送ってもらいます。つまり、途中に信頼できる第三者機関が入るわけです。サトシ・ナカモトが考えたのは、お互いに顔も名前も知らない、信頼関係もないCさんとDさんの間でお金を送れるようにしたいということです。彼が作ったビットコインでは、相手のアドレスさえ知っていれば、直接お金を送ることができ、銀行などの第三者はどこにも絡んできません。

それでは、なぜこのようなトラストレスのシステムが必要なのでしょうか。サトシ・ナカモトの論文には、「誰にも管理されずに、自由に世界中に送金できるようにしたい」と書かれています。ここで「誰にも管理されずに」というのは、政府に規制されない送金システムを作ること、政府の支配が及ばない金融のシステムを作ることを狙ったものと言えるでしょう。このため、ビットコインは、リバタリアン（自由至上主義者）のコインと言われています。その意味で、ビットコインの背景にあるのは、反権力・反政府の思想です。中央政府はろくなことをしない、分散型で民主的にやった方がよいという考えの下に、ビットコインは設計されています。突き詰めますと、アナキスト（無政府主義者）的な発想が背景にあります。かなり危うい発想に基づいてデザインされており、実際にも、中国では、仮想通貨取引所が閉鎖されるまでの二年間、サトシ・ナカモトの思想が実現していたことになります。

(8) 規制の動き

ビットコインは、このような発想に基づいて作られているため、犯罪、マネーロンダリング、テロ資金などに使われたり、非合法決済ツールとして使われたりする可能性が高くなります。

そうなりますと、当然、規制の動きが出てきます。日本では、世界でも最も早く、仮想通貨取引所に登録制を導入しました。問題は、マスコミ報道によって、金融庁がビットコインの取引にお墨つきを与えたと思われてしまったことです。金融庁が認めたから安心だと考えて、多くの人がビットコインを買ってしまいました。

中国では、先ほど申しましたように、仮想通貨取引所は全面的に閉鎖されました。インドでは、仮想通貨取引所は規制されておりませんが、銀行の仮想通貨業者との取引が禁止されています。

今、G20では、仮想通貨をグローバルに規制していこうとする動きが出ています。また、金融庁において、昨年、研究会が設置され、私も委員として意見を述べたのですが、昨年末に、仮想通貨の規制を強化する方向の提言を織り込んだ報告書が取りまとめられました。今年の通常国会に関係法律の改正法案が提出され、規制が強化されることになっています。

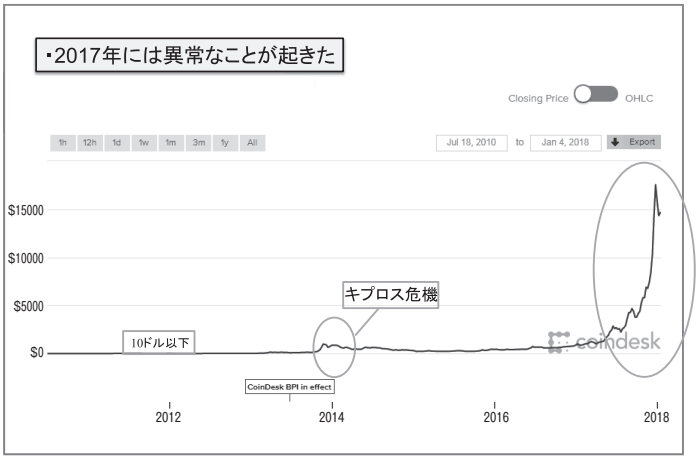
四、ビットコインの将来への懸念

(二〇一七年に起きた異常な動き)

最後に、ビットコインの将来への懸念について申し上げます。

二〇一七年は、ビットコインを巡って相当異常なことが起きた年でした。ビットコインのスタート時からの値動きを見ますと、当初は一〇ドル以下で推移していました（図表2）。ところが、二

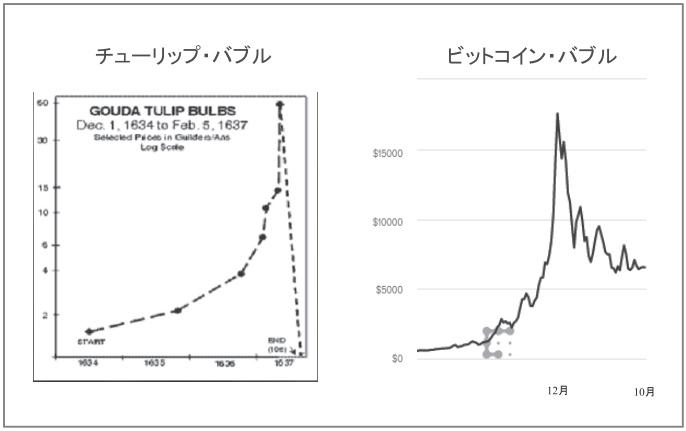
図表２　発行開始からの値動き



〇一三年にキプロス危機が起こり、対応策として、一時的に預金が封鎖され、大口預金への課税が行われました。このとき、預金者が銀行から預金を引き出して、ビットコインを買う動きが広がりました。それにより、一ＢＴＣ一〇〇ドルぐらいであったビットコインの価格が、一気に一〇〇〇ドルぐらいまで値上がりしました。

その後、少し値下がりしていましたが、二〇一七年になって再び異常な上がり方をしました。年初に一〇万円程度であったものが、その後、二〇万円、三〇万円、四〇万円と月毎に一〇万円ずつ上がっていき、一二月に入ったところで一〇〇万円になりました。私は、これはバブルに違いないと考えておりましたが、それから二週間でさらに二〇〇万円まで上がりました。

図表３　２つのバブルの比較



（二つのバブルの比較）

このような価格上昇カーブは、一七世紀にオランダで起きたチューリップ・バブルの最終局面とそっくりです（図表３）。最初は、園芸家が珍しい球根を売買していたにすぎません。その後、ガーデニングに縁のない人たちまで、チューリップの球根の売買で儲けることができるらしいと考えて、チューリップの球根を買うようになりました。その結果、チューリップの球根の価格は、一個で家一軒が買えるところまで上昇しました。しかし、最終局面では、バブルがはじけ、結局元の価格に戻ってしまいました。

ビットコインも、チューリップの球根とほぼ同じようなカーブを辿って、価格が上昇しました。異なっているのは、ビットコインの場合、価格の下落が比較的緩やかであったことです。これは、ビットコインには実需が存在したためではないか

と思います。違法薬物の取引をしている人たちが、コンスタントにビットコインを買っていたため、一気にビットコインの価格が下落しなかった可能性があります。もう一つ異なっていたのは、ビットコインの価格が一定水準以下に下がらなかったことです。これも、買い支えの動きがあったためではないかと思います。

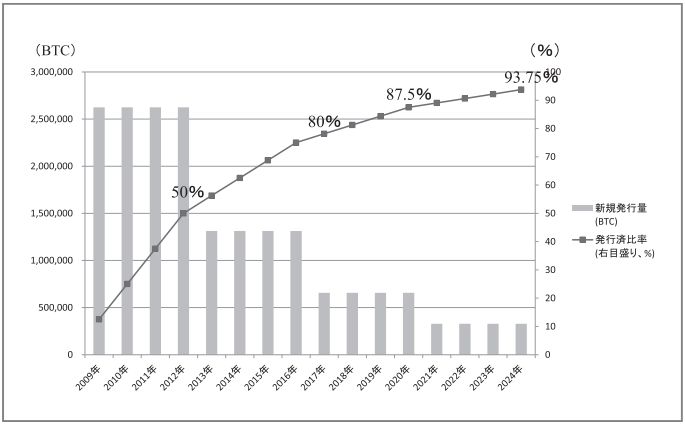
チューリップの球根の価格と、ビットコインの価格の推移を表す二つのグラフを見ておりますと、人間の本質は何百年たっても変わらないと感じてしまいます。いずれも、最初は、わかっている人だけが買っていたわけですが、最後は、わけもわからず、どうも儲かるらしいというだけで、多くの人が買うようになって、バブルが起きてしまうということだと思います。

（リワードの半減期の存在）

もう一つの問題点として、リワードの半減期の存在が挙げられます。ビットコインには二一〇〇万ＢＴＣの発行上限が設定されています。コインの発行量は、この上限に向けて、四年毎に半減していく仕組みになっています。多くの人がビットコインを使うようになって需要が増える一方、時間の経過とともに新たな供給が減少していくわけですから、需要と供給の関係からビットコインの価格は上昇するしかありません。

このことが明らかなので、ビットコインを買わないわけにはいかないということで、多くの人が買いに走りました。その結果、ビットコインは通貨ではなく、資産になってしまいました。もはや誰も、ビットコインを交換手段としては使っていません。金融庁も、仮想通貨ではなく「暗号資産」と呼ぶことになりました。

図表４　ビットコインの新規発行量と発行済みコインの比率



ビットコインの新規発行量と発行済みコインの比率（図表４）を見ますと、ビットコインの発行開始後、最初の四年間で、既に発行上限の五〇％が発行されています。この頃にマイニングを行った人は、大量のビットコインを持っておりますので、大金持ちになっています。その後、二〇一七年末で発行上限の八〇％が発行済みとなっています。

（マイニングの危機）

それでは、今後、ビットコインはどうなっていくのでしょうか。

最初の頃は、マイニングに成功すると五〇ＢＴＣがもらえました。二〇一二年から、これが二五ＢＴＣになり、二〇一六年からは一二・五ＢＴＣまで減っています。これから先も、四年毎に、リワードは、六・二五ＢＴＣ、三・一二五ＢＴＣ、

一・五六二五ＢＴＣと減っていきます。そのような中で、マイナーがいつまでもマイニングを続けてくれるかという問題があります。マイナーは、儲かるからマイニングをしているのであって、人助けのためにやっているわけではありません。マイニングにはかなりの電気代がかかります。このため、マイニングの報酬と電気代を比較して、赤字が出るようになったらマイナーが撤退する可能性があります。そうしますと、取引の承認が遅れたり、ネットワークの安全性が低下したり、最悪の場合、ビットコインの仕組みが維持できなくなってしまったりする可能性もあります。

二〇一八年後半には、ビットコインの価格は、一ＢＴＣが六〇〇〇ドルから六四〇〇ドルを下回ると、上昇に転ずるという不自然な動きを見せました。この水準を下回ると困る人たちがいたのだと思います。実は、マイニングの損益分岐点は六〇〇〇ドルから六四〇〇ドルぐらいではないかと言われています。このため、マイナーが一生懸命買い支えていたのかもしれません。その後、一一月になって、突然、一ＢＴＣ四〇〇〇ドルぐらいまで下落しました。

きっかけは、ビットコインの分裂騒ぎです。二〇一七年八月に、ビットコインのブロックの容量を八メガバイトまで増やせるよう、新たにビットコインキャッシュが生まれました。この他にも、ビットコインゴールド、ビットコインダイヤモンド、スーパービットコイン、ビットコインシルバー、ビットコインゴッドなど、多数の分裂が起こりました。分散型ネットワークで誰もコントロールする人がおりませんので、分裂しようとする動きを止めることはできません。今は、こうした分裂の動きを収拾することができない状況です。

ビットコインの価格低下により採算が悪化したことで、マイナーの間に撤退の動きが起きました。通常、コンピューターは一台、二台という形で売りますが、中国のマイニング・ファームは、不要な装置をキロ単位で投げ売りしたと言われています。日本でも、心配したとおり、大幅な特別損失を計上して、マイニング事業から撤退した業者が出ています。中途半端にマイニングに参入しようとしても、やはり無理だったようです。

（ビットコインに対する三つの懸念）

ビットコインに対する懸念として、三つのことが挙げられます。

一つ目は、匿名性が高いため、どうしても犯罪やマネーロンダリングに利用される可能性が高いということです。

二つ目は、ボラティリティが高いため、支払い手段や価値の保蔵手段など、貨幣としては使えないということです。

三つ目は、ビットコインには、裏づけとなる資産がなく、利子も配当ももらえません。このため、本源的な価値がないのではないかという議論もあります。

（ビットコインのまとめ）

以上で申し上げてきたことをまとめますと、①時々、盗まれたり、なくなったりする、②犯罪に使われている、③規制の抜け穴に使われる、④取引量にも限界がある、⑤電力を浪費している、⑥リバタリアンの思想（反政府・反権力の思想）に基づいている、⑦支払い手段（お金）としては使われていない（投資用の仮想資産になっている）、⑧マイナーがいつまでもマイニングを続ける保証はない、ということが言えようかと思います。

やや時間をオーバーしましたけれども、以上で私の話を終わります。（拍手）

大前常務理事　中島先生、非常に興味深いお話をいただきましてありがとうございました。若干時間を残していただきましたので、御質問等があればどうぞ。

質問者A　マイナーが撤退するとビットコインの仕組みの維持が困難になるというのは、いずれかの時点で取引ができなくなる、ビットコインを持っている人も売れなくなることを意味していると思います。このことがわかっておりながら、なぜ金融庁は登録制のような制度を導入したのでしょうか。

中島　二年前に資金決済法を改正して登録制を導入した際は、フィンテックに仮想通貨が使われる可能性があるため、あまり厳しい規制を導入して、発展の芽を摘んではいけないという考え方がありました。半分は業者育成、半分は規制という感じであったと思います。しかし、今回の金融庁の研究会での議論では、仮想通貨交換業者の中には問題のある業者が含まれており、何か問題が起きると、多くの人に迷惑がかかることがわかってきましたので、規制強化という方向にかじが切られたように思います。

質問者A　ビットコインの仕組みの維持が困難になる確率がかなり高くなってきており、他の仮想通貨についても同様のことが言えるように思います。このため、仮想通貨は、規制するというより、むしろ、禁止すべきではないかと思うのですが、これは過激すぎる考え方でしょうか。

中島　仮想通貨を持っている人は、チキンレースをしているようなもので、最後に暴落するとしても、それまでは値上がりすると予想して、最後の

瞬間に自分がうまく売り逃げればよいと考えているのではないでしょうか。

質問者Ｂ　ブロックチェーンに関し、参加者全員の承認が必要であるため、帳簿を書き換えられるようなことはないと褒めそやされた時期がありました。しかし実際には、ビットコインの盗難など、いろいろな事件が起きています。素人としては、なぜそのようなことが起きるのか素朴な疑問を持つのですが、その点についてもう一度教えていただけないでしょうか。

中島　オン・チェーンとオフ・チェーンは区別して考えなければなりません。

仮想通貨の盗難・流出事件が起きている仮想通貨取引所は、中央集権型の世界に属しており、顧客が持っている仮想通貨を取引所のウォレットで一括して管理しています。そこが破られますと、顧客の仮想通貨は全て盗られてしまいます。ビットコインを持とうとする人が、自分のビットコインを自分で責任を持って管理すれば、このような問題は起きないわけですが、そのような面倒なことはしたくない人は、仮想通貨取引所に口座を作り、パスワードを使って取引をすることになります。取引所が全てを一括して管理しておりますので、そのウォレットが破られますと、何十億円、何百億円という仮想通貨が流出してしまうことになるわけです。

質問者Ｃ　今日のお話の中心はビットコインでしたが、今や二〇〇〇種類ぐらいの仮想通貨が出ています。その中には、ブロックのサイズを大きくするなど、ビットコインの弱みが改善されたものもあります。このような点も踏まえ、仮想通貨全体の将来の可能性についてはどのように考えればよいのでしょうか。合わせて、ＩＣＯ（イニシャル・コイン・オファリング）についてはどのよう

に考えればよいのか、御意見を伺えればと思います。

中島　二〇一七年一月頃は、仮想通貨全体の九〇％がビットコインでしたので、仮想通貨＝ビットコインという感じでした。その後、ビットコイン以外の仮想通貨が次々に出てきまして、今は、ビットコインが四〇から五〇％、残りの半分がイーサリアム、リップルといったアルトコインになってきています。これらの新たに生まれた仮想通貨の中から、新しいブレークスルーが生まれる可能性は否定できず、仮想通貨の全てがダメだと決めつけるつもりはありません。

なお、ビットコインのデザインは全てインターネット上で公開されています。新しい仮想通貨の多くは、それを基に、一部を修正した形でできあがっています。互いに似ておりますので、ビットコインと同様の問題が他の仮想通貨でも起きる可能性はかなりあるのではないかと考えています。

ＩＣＯについては、昨年の金融庁の研究会においても、いろいろな議論がありました。ＩＣＯに関しては、その内実をよく知っている人ほど反対する傾向があります。逆に、よく知らない人は「これは新しい資金調達の手段だから、なるべく生かしたほうがよい」と言いがちです。ある調査によれば、ＩＣＯの八割は詐欺であると言われています。事業をやるつもりがないのに、もっともらしい計画を示して資金を調達しているわけです。また、残りの二割がまともかと申しますと、必ずしもそうではありません。単に「ブロックチェーンを使って世界を変えたい」といった提案書を出して、資金を集めているものが多いようです。このため、ＩＣＯは、まともな資金調達手段としてはほとんど機能していないのでないかと思います。金融庁の研究会でも、私は、ＩＣＯを規

制すべきという立場で意見を述べました。今回の見直しでは、株式類似のものは金融商品取引法で規制し、それ以外のものは資金決済法で規制する方向で整理されています。

大前常務理事　予定の時間を過ぎておりますので、今日の講演会はこれで終わらせていただきます。

中島先生、どうもありがとうございました。

（拍手）

（**なかじま　まさし・麗澤大学経済学部教授　早稲田大学非常勤講師**）

（本稿は、平成三一年二月二〇日に開催した講演会での講演の要旨を整理したものであり、文責は当研究所にある。）

中　島　真　志　氏

略　　歴

81年一橋大学を卒業し、同年日本銀行に入行。

調査統計局、金融研究所、国際局、金融機構局、国際決済銀行（BIS）などを経て、現在、麗澤大学経済学部教授。早稲田大学非常勤講師。博士（経済学）。

単著に『SWIFT のすべて』、『外為決済と CLS 銀行』、『入門 企業金融論』、共著に『決済システムのすべて』、『証券決済システムのすべて』、『金融読本』（いずれも東洋経済新報社）など。

決済分野を代表する有識者として、金融庁や全銀ネットの審議会などにも数多く参加してきており、昨年は「仮想通貨交換業等に関する研究会」（金融庁）のメンバーを務めた。

最新刊の『アフター・ビットコイン』（新潮社）は、仮想通貨とブロックチェーンを扱った一冊として注目を集め、約５万部のベストセラーとなっている。