

「石貨・仮想通貨・ブロックチェーン」

早稲田大学 商学学院教授 佐々木 宏夫

石貨からブロックチェーンへ：

ただいまご紹介いただきました佐々木でございます。今、高瀬所長から非常に質の高い難しい議論が展開するであろうということをお話いただきました。実際、私どもも事前に皆さんといろいろやりとりいたしまして、最先端の非常に面白いお話をたくさんいただけたと思います。

私は、最初に前座というかイントロでございますので、ウォーミングアップということで、そんなに難しい話ではございません。むしろ、先ほど高瀬さんがおっしゃっていた南の島の石貨の話から、それがどうしてブロックチェーンにつながっていくのかという、その辺りの話をまずさせていただいて、その後は少し難しい話がそれぞれの皆さんから続くということになるかと思います。

それです、突然こういう地図を出すのも恐縮なのですが、これは日本の南側の太平洋エリアの地図であります。ここが日本ですね。日本の南にグアム島がございます。そこからさらに南に下った所に、このミクロネシア連邦という四つの大きな島を中心にして成り立っている島嶼国がございます。その国の一番西の端の大きな島がヤップ島という島でして、この島が実はこれからお話しする物語の原点でございます。

ヤップ島というのは、これはミクロネシア大使館の地図から取ってきたヤップの地図でございますけども、だいたい人口が1万人ちょっとの島で、サイズとしては伊豆大島とほぼ同じぐらいの大きさの島であります。ですからそんなに大きな島ではないですが、ミクロネシア連邦の中では大きな島であります。

ミクロネシアは白人が来る前は、地元の人たちが普通に統治していたわけですがけれども、その後スペインが来て、ドイツが来て、この地を支配し、さらに第一次大戦が終わったときに国連の委任統治領ということで日本の領土になりました。そして第二次大戦後はアメリカの信託統治領になり、そして1986年に独立して91年に国連に加盟したという国です。

ヤップ島には、非常に有名な石の貨幣があります。これを地元の人々は、「フェ」とか「ライ」とか呼んでおります。

この写真は、今年の3月に何人かの共同研究者たちとヤップ島に行ってみまして、そこで撮ったものです。ご覧になればおわかりのようにかなり大きなものです。大きさを実感していただくために、次の写真を置いてみました。ここに写っているのは、今回の旅で一緒した神戸大学のS先生なのですが、彼の身長と比べてもどれぐらい大きいかということがお分かりになるかと思います。

この石の通貨が、実は何人かの非常に優れた経済学者たちの注目を集めました。1人はジョン・メイナード・ケインズであり、もう1人がそのミルトン・フリードマンであります。彼らはこれが世界の信用通貨のある意味で原点なのだ、というようなことを言ったわけであります。

今でも、実はこの通貨は機能しております。例えば、結婚のときの、日本でいう結納金に当たるようなお金であるとか、けんかしてお詫びに行くときの仲裁金に使うとか、土地の売買のときに使うとか、そういう目的で今でも機能している通貨であります。

ただ、こんなに大きな石であります。とてもでないけれど持ち運ぶことはできないわけです。もちろん小さな石貨の場合には持ち運ばれることもあります。この写真は3月にヤップに行ったときに見せてもらった伝統的な行事なのですが、小さな石を誰かに渡すときにはこういうふうに行列をつくって移動させることもあるようです。ただし、大きな石貨はそういうわけにはいかず、この写真にあるように村のある場所に固定しておきます。ただしこの石は、必ずしもその村の人の持ち物とは限りません。ヤップ中のいろいろな人に所有権があるわけであります。

それでは、なんでこういうものが通貨としてそれなりに機能してきたのかという、そのあたりがまずわれわれにとっての非常に大きな疑問になってくるわけです。実はこのヤップの通貨というのは、なかなか面白い特徴を持っております。

まず、もともとヤップ語には文字がありませんでした。ですからさまざまな情報は人々の記憶の中にとどまっているわけでありすけれども、実は石貨についても同様に、各石貨には、固有の歴史があります。ヤップの多くの人々は、その石の歴史を知っているわけであります。

石貨の価値はどのようにして決まるのかと言うと、その石の歴史と実は関連しています。つまり非常に苦労して獲得された石の貨幣は価値を持ちます。苦労していないものはあまり価値を持ちません。ヤップからさらに西に450キロぐらい離れた所に、パラオというダイビングなどで有名な島があります。ヤップ島の、先ほど写真を見ていただいた石貨はパラオで造られて数百年前にカヌーに載せて運ばれてきたものです。これを運ぶ旅は恐らく大変な苦労を伴っていたらと思います。

しかも運ぶ途中でいろいろな問題が起きるわけですね。嵐に遭っていったん沈んでしまって、海から引き揚げられたなどという石貨もあるかもしれません。こういう石は、ものすごく価値を持ちます。非常に簡単に手に入った石は、実はあまり価値を持ちません。ですから非常に面白い話がありまして、ドイツの統治時代にあるドイツ人が、確かオキーフという名前のドイツ人でありすけれども、機械を使って非常に形の美しい石貨を大量生産しました。今でも一部残っているようですが、これには全く価値がありません。それはなんの苦労もないからであります。こういう石貨に関する歴史の記憶、それに加えて取引記録、これが実は人々の頭の中に共有されているというのがヤップの通貨の仕組みであります。

そうなる一つ疑問に思うのは、その取引記録は改ざんされたり不正に使われたりすることはないのだろうかという疑問です。実際、例えば誰かに石貨を何十年前かにあげただけで、そんなことはしていないよというような人が出てくるかもしれない。そういうときにどうやってその問題を

阻止するのかというと、ヤップというのは小さな島ですから、取引の記録というのは全ての人々の頭の中に共有されております。しかも、語り部のように記憶力のいい人もいた可能性があります。それに加えて、そもそも今でもテレビのないような島でありますから、人々の関心の対象は非常に限定されているわけです。

だからその石が誰それぞれの所に渡ったはずだという記憶は、他の人たちの記憶の中に全部とどまっています。そうすると、仮に誰かがズルをしようとしても、おまえ、そんなうそ言っちゃ駄目だよ、この石はいついつにこういう経緯でおまえからあの人に渡しただろうということになってウソがばれてしまうわけです。そういう形でうそや改ざんを阻止するという仕組みになっております。

ヤップというのは、ミクロネシアの中でも面白い歴史を持っている島でありまして、先ほど言ったミクロネシアの四つの大きな島のうちの二つの島には、実はスペイン人が来る前にはかなり中央集権的な王権が成立しておりました。ところがヤップは、実は極めて分権的な社会であります。今でもそうですけど、最近はず長という言葉を使っちゃいけないようなのでチーフと言いますが、何人かの村を支配するチーフがいて、その連合政権みたいなものです。しかも、村同士はそんなに仲よくありません。ですからよく村戦争などが起きる。このようにヤップというのは極めて分権的な社会であります。

そういう分権的な社会で、なぜ通貨の信認が保たれたのかというのが、実は一つのパズルであります。確かに中央集権的な、日本で言えば日本銀行みたいなものがあれば、そこがこれは価値があるよと宣言すればそれで価値があるわけですが、実はヤップの通貨の場合は全ての人々の目にさらされて、誰かがうそをついたらそれをリジェクトするような力が働くというその構造が、実は信用を確保しているのであります。だからちょっと模式的に書けばこういうことで、要するにこの2人が石貨の取引をしたとしたら、それをみんながチェックしているわけですね。みんなの頭のデータベースの中に、その取引記録が刻み込まれているわけです。そうするとそこでその当事者のうちのどちらかが後になってごまかそうとしても、実はそれが許されないという、そういう仕組みになってきております。

それでは、なんで石貨の仕組みはうまく機能したのかといいますと、今幾つか申し上げましたように、一つには小さな社会だったこと。せいぜい人口1万人ぐらいの社会であります。それから、そこに意外と分権的ではあるのですが、村と村とを結ぶ、情報伝達経路があったのだということも知られております。それから、人々の関心が非常に限定され、テレビもないわけですから、だからやっぱりみんなが鵜の目鷹の目で他の人の様子を見ているわけですから、記憶が共有されやすいという特徴もあります。それから、経済自体の規模が非常に小さいという、そういう特徴がございます。だからうまく機能したわけです。だから日本で同じシステムが機能するかというと、基本的には無理なわけですね。ただ、そこでわれわれがテクノロジーの進歩というものを考慮に入れると、その無理が可能になったというのが、今日の報告者の皆さんのお話になるわけです。

ブロックチェーンの仕組み：

つまり、コンピュータの中に記憶をとどめておけば、記憶の劣化は起きません。先ほどのいろいろな人間の目の代わりに、沢山のコンピュータの中に同じような情報のセットを入れておけば、どこかで何かの不正や改竄などが生じても、すぐ見破られてしまいます。これが石貨の仕組みを現代的に生かすための基本的な道であります。

そういう点で、先ほど述べた石貨の教訓を整理しておきますと、一つはヤップの石貨の場合重要なのは、苦勞を伴わないと価値を持たないということです。これは通貨が通貨として機能するためには非常に重要な条件であります。実はビットコインなどの場合には、同様の「努力」は、採掘（マイニング）という無駄な計算をさせること——まるでシーシュポスの神話のような——で行われています。

第二に、現在の管理通貨制度というのは、国家が自分の権力を使って苦勞を代替している仕組みだというふうに理解することもできるかもしれません。それに対して、石貨もブロックチェーンも基本的に多数決原理で物事を考えるわけです。このような多数決原理などで意思決定を行う手順を「合意形成アルゴリズム」と呼びます。つまりこれは、みんなが同じ情報を共有していると、誰かが逸脱行動をしたとしても多数決で封じ込めることができるという、そういう仕組みになっているわけです。しかも、皆が同時に保存するデータセットの中身は歴史的な記録です。それをずっと保存しておくわけです。ヤップの通貨においては、過去の石貨の政策や運搬、あるいは取引の歴史がそのまま残っているわけです。実は歴史的データを保存しておく、どこかでうそをつこうとするとずっと連鎖的にうそが累積してくという問題が出てきて、結局うそがつけなくなるわけですが、この話は後でいたします。

今まとめたような石貨の仕組みを、現代のシステムの中に埋め込むと、意外とうまくいくのではないか、というアイデアが出てくるわけであります。

ここでいよいよビットコインやブロックチェーンの話が出てくるわけです。ビットコインについては、ご存じの方も多いと思いますけど、どういう人かは分からないサトシ・ナカモトと称する人の2008年の論文が出発点だったと言われてしています。

もともとその論文の中では、ビットコインのアイデアとブロックチェーンのアイデアが混然一体として出てきたおりました。ただし、少し詳細にサトシ・ナカモトの論文を検討してみますと、必ずしもそのブロックチェーンというのはビットコインだけを支える技術ともいえないだろうということが分かります。ビットコインはあくまでも「一つの」仮想通貨に過ぎないのですが、ブロックチェーン技術の応用範囲はビットコインだけに留まらないのです。

そういう点で、ここでもあえてビットコインのシンポジウムではなくて、ブロックチェーンのシンポジウムというのをやってみようというふうに思ったわけです。

それでは、現代の日本のような「大きな」社会でどうやってうそを阻止するのかというと、先ほ

どの絵、ヤップ島でのコミュニケーションのスライドにおける人々を、コンピュータに置き換えればいいのです。このネットワークの中でお互いが同じようなデータセットを持つことによって改ざんを阻止しようという、そういう仕組みになると思います。

ですから、ここで少し整理しておきますと、今度は現代のシステムとして機能させる場合にも、ヤップの石貨と同様にその歴史的な経緯を全て記録するということが必要です。それからあとは、誰に記録を台帳に追記する権利を与えるのかについてのルールをちゃんと作っておきましょうということも大切です。このルールが合意形成アルゴリズムなのであります。それから非常にたくさんのコンピュータの中に、同じようなデータセットを保管しておくことによって、改ざんや不正を阻止するような仕組みができるでしょうということです。

このスライドはちょっと面白おかしく書いたのですが、要するに、なんで歴史的なデータを全部保全しておく必要があるのかということをこのスライドは示しています。例えばビットコインで言えば、2008年の論文によってビットコインが生まれて以来の取引記録は、ずっと保管されているのです。これはなぜかと言うと、過去にさかのぼってズルをするやつというのが出てくる可能性があるからです。そういうときに、過去からのデータを保全しておく、そこをいじろうとすると今のデータが実は違ったものになってしまっていて、そこでうそがばれるという、そういう仕組みを使っているわけですね。

ですから、次のたとえ話で良く理解できると思います。タイムマシンで過去に行ったときに、その歴史を変えるようなことはしちゃいけませんよという話があります。例えば誰かがタイムマシンで過去に行って、戦国時代あたりで別の武士と決闘して相手を斬り殺してしまったとします。ところがそうすると、その途端に自分自身が消滅しちゃうんですね。なぜかと言うと、実はこの殺した相手は自分の先祖だったのです。先祖を殺してしまえば今の自分は存在できないわけです。つまり、過去をいじるということは今に必ず影響があるわけです。そういう点で歴史的なデータを保存するというのは重要なのであります。

それからもう一つ、これはヤップの通貨を超えた技術ではありますが、「暗号学的ハッシュ関数」とか、単に「ハッシュ関数」と呼ばれている技術を使って、うそを見破ろうとする工夫がブロックチェーン等々ではよくやられております。

これは何かということを簡単に説明しておきますと、まず「関数」というのは、あるインプットに対して、あるアウトプットを出すような、そういう数学的な関係のことを言います。インプットとしていろいろなデータを入れてみましょう。データというのは、基本的に文字列であります。その文字がコード化されていれば、データは数字の列であります。このインプットされたデータに対して、ある桁数の数字をアウトプットするような関数がハッシュ関数であります。

これだけでしたら、関数と呼ばれるものはみんな同じであります。ただ、ハッシュ関数の場合は、通例は、256ビットの数をアウトプットすると。ただ普通は16進数で書きますので、256ビットということは2進数で256桁ということですから、16進数で言えば64桁の数字をアウトプットする

のです。もっともこのアウトプットの桁数については今後増やされる可能性はあります。そして、このアウトプットした値のことを通例はハッシュ値と呼んでいるわけです。

ところが、このハッシュ関数というのは単純にその 64 桁の 16 進数をアウトプットするだけではなくて、非常に面白い特徴を持っています。例えば今このスライドに書いてあるのは、現在比較よく使われているそのハッシュ関数のアルゴリズムを使って、私の名前をアウトプットしたものです。つまり「佐々木宏夫」という 5 文字をアウトプットして、64 桁の 16 進数にしたのがこれです。この数字列は、わけの分からない文字の並びになっております。これがみそでありまして、実はハッシュ値というのは、基本的にちょっとでもデータを、たとえば佐々木宏夫の「夫」を、夫でなくて「雄」にただけで全く違う文字の並びになってしまうという性質を持っているのです。

ですから誰かがちょっとだけデータを改竄したとしても、ものすごく大きなデータでしたら、すべてを比較して改ざんがあったかどうかをチェックするのは大変ですが、たった 64 桁の 16 進数を比較して、それが大きく変わっていれば、これはなにか変更があったのだということがたちどころに分かるのです。

それから、理論的に言うと、異なる入力データに対して同じハッシュ値が出てくる確率は 0 ではありません。ただ、その確率が非常に小さくなるようにハッシュ関数は作られているのです。それから、入力データからハッシュ値を予想することができないというのも重要な性質です。

実は、ビットコインにおけるマイニングの基本的な原理はこのハッシュ関数の性質に基づいています。マイニングということで具体的に何をするのかというと、0 が最初の何桁も並んでいるようなハッシュ値を出すための計算競争をさせるわけです。ところが先ほどのハッシュ関数の性質から分かるように、どういう入力データを入れたらゼロがたくさん並ぶのかということは誰も分かりません。ですから、必死になってでたらめに数を入れるわけです。そしてだいたい 10 分ぐらい計算したら、0 の並びが十何桁の 0 というハッシュ値が出てきます。そういう競争をさせて勝った人が台帳に記載する権利を与えられる人になるという、のがビットコインの合意形成アルゴリズムです。そういったこともハッシュ関数を使うとできるのです。

次にブロックチェーンについて考えてみましょう。長い期間にわたって每期取引が行われるわけです。例えば、住宅ローンを組みましたとか、何かを買いましたとか、こういう取引が日々行われ、台帳に記載されるわけです。ブロックチェーンの「ブロック」というのは、毎期のそのような取引記録と後で述べるやり方で計算されたハッシュ値が少なくとも記録されているデータの塊（つまり、ブロック）です。それが、時間の経過にしたがって鎖のようにつながられていくので、ブロックチェーンと呼ばれるわけです。

各ブロックに記載されるハッシュ値はどう計算されるのかというと、それはその前の期のブロックに記載されているデータのハッシュ値です。前の期のブロックの中には、その時行われた取引のデータとさらに一期前のブロックのハッシュ値が入っているのですが、これを合わせてインプットして、アウトプットとして得られたハッシュ値を今期のブロックに置くわけです。

こういうブロックにデータを置くと、なぜ改ざんができないのかといいますと、私が例えば30年前に組んだ住宅ローンの記録を消してしまったとしましょう。そうすると、30年前のブロックの中身はちょっとだけ変わります。その途端に、そのブロックのハッシュ値が大きく変わります。そうすると次の期のブロックに記載されるハッシュ値が変わります。さらに次の期のブロックの中身が変わりますから、その次の次の期のハッシュ値も変わります。……。こういう事がずっと繰り返されて、今のハッシュ値も変わってしまいます。

そして、今のハッシュ値をお互いが比較すれば、私が持っているデータ（ブロック）だけは違うハッシュ値を持ってしまうから、そこで「ああ、こいつ悪いことしたな」とばれてし舞うわけです。

いまブロックチェーンの基本的なアイデアをご紹介しましたが、このフォーラムではこれから先はたぶん難しい話になるかと思いますが、金融や市場の設計、あるいは社会的なインフラ整備など、さまざまなところでブロックチェーンの技術は活用できるということをお話したいと思っています。

その後で法的な論点についてお話いただき、さらに私自身経済学者の立場からブロックチェーンの問題点や可能性などについてお話ししたいと思っております。

2分ほどオーバーしてしまいましたが、一応私のほうからはイントロダクションとしてのお話をさせて頂きました。どうもありがとうございました。