ISSN 1343-9561

R.I.B.A. ACADEMIC FORUM

No.25

第 25 回　産研アカデミック・フォーラム
「ブロックチェーンが切り拓く未来」

2017
早稲田大学産業経営研究所
Research Institute of Business Administration

第25回　産研アカデミック・フォーラム

ブロックチェーンが切り拓く未来

2017年５月13日（土）

於：早稲田大学　大隈記念講堂小講堂

◇ 目　　次 ◇

※講演２につきましては、企業情報が含まれておりますため、非公開とさせて頂きます。

ご　挨　拶

早稲田大学　産業経営研究所　所長、商学学術院教授　**高　瀬　浩　一**

早稲田大学産業経営研究所所長の高瀬浩一と申します。産業経営研究所、略して産研は、学術と実業の懸け橋となる機関として早稲田大学商学部、大学院商学研究科、会計研究科の教員を中心とする研究員が、ビジネスに関わる研究、研修支援、研究成果・研究フロンティアの発信・公開に務めております。これまで公開講演会を始め、春の産研アカデミックフォーラムと秋の産研フォーラムを定期的に開催してまいりました。今回、第25回産研アカデミックフォーラム「ブロックチェーンが切り拓く未来」を開催することになりました。皆様、ご参集いただき、誠にありがとうございます。

今回は、特に高度な内容を想定し、定員人数をあえて絞り、高い意識と一定以上の基礎知識を持った聴衆の方を前提にしています。皆さん、覚悟を持って臨んでください。

今回のテーマは、実は世話人である、私の同僚の佐々木教授との会話がきっかけとなりました。ある日、佐々木先生が私の研究室に来て「ビットコイン、仮想通貨の発想の原点って知ってる？」。それから「高瀬さん、知ってる？　マイニングはね」「高瀬さん、知ってる？　ブロックチェーンはね」。こういうのを何度も繰り返し、結局、「次の産研アカデミックフォーラムは仮想通貨でやろうよ。ブロックチェーンがあんまりにも面白いので、仮想通貨だけではもったいないからブロックチェーンとの２本立てにしましょうよ」っていうことで決まりました。

ちまたでは、ブロックチェーンはメディア一押しの話題だと思います。最近の日経新聞見開き１ページで、あるいはNTTのWeb特集で。日刊工業新聞電子版「ゴールドラッシュ前夜迎える。ブロックチェーン」。仮想通貨、ビットコインに至ってはバブル状態ですね。過熱する仮想通貨、投資セミナー、コイン取引所障害。ここで共通の疑問が皆さんにも湧いてきますよね。われわれは何を知っているのか。みんな、どこまで分かっているのか。このような点が今回のテーマになっています。

佐々木先生によるご講演者の地道なかつ着実な探索とご依頼、ご講演者との幾度とない打ち合わせを行って、金融企業、IT管理、暗号技術、電子商取引法のそれぞれの分野で最高の講演者を準備できました。講演者の皆様、ご所属先のご関係者の皆様のおかげです。心より感謝申し上げます。

最後に、この場所です。大隈重信が在野の精神、学の独立を標榜し、早稲田大学を設立しました。建学の精神は130年以上、現在まで引き継がれ、この大隈記念小講堂の名前の由来ともなっています。権力や政権におもねることなく、可能な限りの情報提供と自由闊達な議論を、主催者側として保証したいと思います。

今日は日本と世界の経済社会の将来について、皆で考えていきたいというふうに思っています。今後も産研では、日本の金融政策、保険アクチュアリー、日中経済交流、企業経営など幅広いテーマについて公開講演会を開催、企画していきます。ご期待ください。

それでは、これをもちまして、あいさつと代えさせていただきます。どうもありがとうございました。

2017年5月13日（土）

イントロダクション：
ブロックチェーンとは何か

「石貨・仮想通貨・ブロックチェーン」

早稲田大学 商学学術院教授　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しいただきました。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ると思います。

私は、最初に前座というかイントロでございますので、ウオ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。

それでまず、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まいりまして、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、今回の旅でご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ございませんでした。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ますけれども、実は石貨についても同様で、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だろうと思います。

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ますけども、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けど、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。

そうなると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のだけど、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さん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、最近は酋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けども、何人かの村を支配するチーフがいて、それ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けれども、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。先ほどのいろん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、苦労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労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と、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ると思います。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ましょうという、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ね。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と、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、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おります。例えば今このスライドに書いてあるのは、現在比較的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あります。これの数字列は、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」にし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、これはなにかか変更があったのだということがたちどころに分かりるのです。

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らない。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毎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げられていくので、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いますから、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けれど、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いただきたいと思います。

その後で法的な論点についてお話しいただき、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けど、一応私のほうからはイントロダクションとしてのお話しをさせて頂きました。どうもありがとうございました。

第一部：
ブロックチェーンの活用

講演 1

「銀行におけるブロックチェーン技術の活用可能性と課題」

三井住友銀行 IT イノベーション推進部　竹田　達哉

三井住友銀行 IT イノベーション推進部の竹田です。私どもの部署は三井住友フィナンシャルグループ全体の金融をスコープにしておりまして、金融分野におけるイノベーション創出をミッションとしている部署です。IT、IoT ですとか AI、本日ご説明しますブロックチェーンなどの要素技術、テクノロジーを用いて、新たな金融サービスづくりをしています。

金融の分野において、ブロックチェーンは新たな要素技術として世界中でいろんな試行ですとか開発の競争が行われています。今日は日本の金融機関が、現時点でブロックチェーンの有効性をどのように見ているか、どのあたりが実用にできるのかとかいうことを、技術にあまり深入りすることなく、実務の立場からお話ししたいと思います。先ほど佐々木先生から、これから難しくなりますというお話がありましたが、私のところはまだ簡単だと思いますので、気楽に聞いていただければと思います。

今日のマテリアル、お手元に配っているものあるかと思いますが、これは 3 月の 16 日に全銀協が公表した「ブロックチェーン技術の活用可能性と課題に関する検討会報告書」というものをベースにしておりますので、詳しい内容をご覧になりたい方は全銀協のホームページ見ていただければ PDF で載っておりますので、そちらをご覧ください。

まず初めに申し上げておきたいのですが、ブロックチェーンは世の中を変える技術であるということで、夢が先行している感があるのではないかなというふうに、私自身思っています。世の中を変える技術であるかどうかというのは、私自身まだ確信には至っておりません。この後、各分野の先生方がブロックチェーンについてさまざまな角度からお話しされると思いますので、私自身も理解を深めたいなと今日は思っております。

今日の流れですけども、簡単にブロックチェーン、先ほど佐々木先生もご説明されていましたので、簡単にですがおさらいをして、そこからブロックチェーンの要素技術、ブロックチェーンの形態、活用分野の検討、活用上の論点、さらに個別の金融における論点、あとブロックチェーンが適する金融上の業務、取引、あと課題、そういったところをご説明していきたいと思っております。

「ブロックチェーンとは？」ということで簡単におさらいでございます。ブロックチェーンとは簡単に言いますと、信頼できる台帳を中央機関なしで成り立たせる技術ということです。もう少し別の言い方で言いますと、取引履歴を暗号技術によって過去から 1 本の鎖のようにつなげる、ある

取引について改ざんを行うためには、それより新しい取引について全て改ざんしていく必要がある仕組みということです。これによって正確な取引履歴を維持しようとするインセンティブを与える技術であるというふうに言えます。

ブロックチェーン技術には、ビットコインをはじめとします仮想通貨の技術基盤である狭義のブロックチェーン技術と、目的に応じてブロックチェーンの技術的特徴を部分的に取り出した広義のブロックチェーン、これはいわゆる分散型台帳と言われていますけども、この二つがあると言われておりまして、技術者の方々に言わせると、ブロックチェーンと分散型台帳の技術は違うのだということで、そこだけで長い議論がされるのですが、今日はブロックチェーンと分散型台帳技術、これまとめてブロックチェーンというふうに言うことにします。

ブロックチェーン、何が新しいかと言いますと、従来は銀行を含めまして中央の管理型のシステムで取引履歴を管理して、信頼性を担保しているということです。これをブロックチェーンでは分散管理システムで全ての取引履歴をみんなで共有するということで、信頼性を担保するというのはブロックチェーンの新しさであります。

これは突き詰めていきますと、信頼性をどこに求めますかという、これまでの国を信用してればいいとか、銀行を信頼してればいいという、そういう発想を大きく変えるものであると思います。信頼できる第三者機関を置かずに、台帳の整合性ですとか、改ざんを防止することを実現するということで、革命的な技術として注目を集めています。

ブロックチェーン技術の優位性としましては、改ざんが極めて難しいということ、あとデータが消失しないということ、コストが削減できる可能性があることというのがメリットとして言われております。一方でブロックチェーン技術の課題としましては、取引の確定までに時間がかかること、ブロックチェーンの性能や仕様がまだ十分ではないことがあります。これらの点は今日お話しする中で、何度か強調することになりますので覚えておいていただければと思います。

こちらのページ、ブロックチェーンをもう少し細かく書いたものですけれども、こちらは後ほど先生方が詳しく、ブロックの形成ですとか暗号取引のことについてはお話されると思いますので、このページは私のほうからは割愛させていただきます。先ほど佐々木先生から話があったハッシュ値の考え方なんかは、こういったところに出てきております。

ではここから、実ユースにおけますブロックチェーンの活用についてご説明をいたします。ブロックチェーンには幾つか要素技術が使われております。ここに載せている五つになります。

まず分散型台帳の技術ですけれども、これは通常の集中管理型のシステム、例えば日銀ネットですとか、中央銀行の決済ネットワークと異なりまして、P to P、Peer to Peer のネットワークの参加者によってそれぞれ保持されるというものです。ここでいう Peer to Peer のネットワークとは、例えば個人の持つ PC も Peer になり得ます。すなわち中央集権型であれば銀行のサーバーに情報を見に行くわけですけども、分散型台帳システムでは個人の持つ PC でデータをみんなで持っているということです。それぞれの自分の PC、他の方の PC を見に行くということです。

３番目の偽造防止暗号化技術ですけども、これは取引情報をネットワーク上に流す際に自らの取引であることを証明するために、公開鍵暗号方式を用いて電子署名すると。それで、ハッシュ関数で計算するといった、先ほどあったような方式が使われているということであります。

４番目のコンセンサスアルゴリズムですけども、これはちょっと重要な概念ですので後ほどもう少し詳しくご説明します。

最後に、スマートコントラクトですけども、定義としましてはプログラム化されて自動的に執行可能な契約ということで、今ここでは細かく触れませんが、これも重要なポイントになってきますので後ほどご説明します。

６ページですけども、ブロックチェーンには参加者の公開範囲ですとか制限内容によって、三つのタイプがございます。パブリック型とコンソーシアム型、プライベート型の三つでございます。これらは、実際利用するケースに応じてそれぞれ適切な形態が選ばれるということに現状なっております。真ん中のところにありますコンセンサスアルゴリズムですけども、これは単純に言いますとブロックチェーン上の物事の決め方、ガバナンスということになります。大きく管理主体が存在するのかしないのかによって分けられます。

例えばビットコインのブロックチェーン、これはパブリック型の代表なのですが、ビットコインブロックチェーンに使われるコンセンサスアルゴリズムはプルーフ・オブ・ワークと呼ばれるものです。これは多大な計算を必要としますので、この計算量が必要な問題を最初に解いた人、すなわちこれマイナーですけども、最初に解いたマイナー、ワークした人がブロックを形成する権利を得て、ビットコインを受け取るということです。

ビットコインブロックチェーンの場合、マイニングに成功して次のブロックを形成するまでに約10分間要するというふうにプログラム上設定されておりますので、従って10分間は取引が確定しない、タイムラグが生じるということでリアルタイム性が欠けるという弱点があります。またこの10分間に同時に複数のブロックが形成されるというケースもありますが、この場合、ルール上より長いブロックが優先されるということで取り決められているのですが、いずれにしても最終的に取引が確定するまでに時間がかかるという弱点があります。

あと右側の二つ、参加者が限定されるコンソーシアム型ですとかプライベート型のブロックチェーンでは、BTFTといったコンセンサスアルゴリズムが使われます。これはネットワーク上に参加者の１人をリーダーとして、自らを含む全参加者に要求を送って、その要求に対する結果を集計して多数を占める値を採用するとうことでブロックを確定させる方法です。従いまして、中心になるリーダーと呼ばれる人がいるということです。

ここで皆さん、はてなと思ったかもしれないのですが、「もともとブロックチェーンというのは、中央管理者はいないのでは？」ということを思ったのではないかと思います。コンソーシアム型ですとかプライベート型は本来的なブロックチェーンの要件を満たしているのだろうかというのは、これリーダーがいるのであればクラウドサーバー使うのと何が違うのかという点は、皆さん思うと

ころかと思います。この点今後、ブロックチェーンを使っていくに当たって思想の問題にもなると思うのですが、中央管理者がいる、いないと、これ今、二つのパターンご紹介したのですが、そこを論点とするのではなくて台帳として改ざんできないということが、ブロックチェーンの存在意義なのではないかというふうに考え始められています。コンセンサスアルゴリズム、これは先ほど申し上げたように、ブロックチェーン上の意思決定のガバナンスが大きな問題にこの後なってくるということです。

改ざんできないことがブロックチェーンの存在意義であるかもしれないにもかかわらず、これはまた後ほど先生方からお話あるかもしれないのですが、昨年イーサリアムというブロックチェーンがハードフォーク、ブロックの強制的な書き換えというのを行いました。今今現在は、ビットコインブロックチェーンが仕様の変更をする、しないということで、コミュニティが二つに分かれていると状況になっていまして、ビットコインブロックチェーンの２というのが出てくるかもしれない状況に陥っています。それで、ビットコインの事業者の方々に聞くと、本当にビットコインブロックチェーンがなくなってしまうかもしれない、今危機的な状況であるというようなことを言っておりました。こうなりますと、ガバナンスの安定性ということで金融などではなかなか使いにくいというのがまだ現状あるというふうに考えております。

あと細かいのでお手元の資料見ていただければと思いますけども、こちら、現在金融分野においてブロックチェーンが活用できるのではないかと考えている分野です。通貨、送金決済、貿易取引ですとかシンジケートローンの融資の分野、あと株式ですとかデリバティブといった金融商品取引、あと一番下のところですが、本人確認作業のような金融情報管理で実証実験がいろいろ進められているということでございます。

では、ここまでの過去数年間、実証実験などで実際にブロックチェーン、私自身も触っているのですが、金融の分野でどのような点が論点になっているかというところをご説明します。議論の前提として、これはよく議論になるのですが、そもそも既存または新たに開始する業務、取引について、中央で管理するシステムとブロックチェーン、いずれが適するかというような、常に置き換えの議論というのはあるのですが、そこは業務ですとか取引ごとに性質や特性が異なっているということは頭の中に入れておく必要があります。

現在、銀行業務取引は中央集権的に中央管理のシステムで管理されることが一般でありますので、すぐにある業務に関してブロックチェーン技術を使うかどうかというのは、よく検討して比較する必要があるということがあります。

論点、順番にご説明しますが、まず機能の面です。性能要件、データの同期の問題でファイナリティというのが論点になってきています。ブロックチェーンの要素技術であります先ほどのコンセンサスアルゴリズム、あとはアルゴリズムの処理の速度というのは、これ結果として処理の性能を決める要因になってくると。10 分間ファイナルされないとかというのは要因になってくると。遅過ぎると性能要件を満たさないで、速過ぎるとブロックチェーンの処理にシステム上の負荷が大き

くなってくるという論点があります。

このネックを解消するためには、コンピュータの性能は日々上がっておりますので、性能の向上によって処理性能を改善していく必要というのはあるのですが、単位時間当たりに共有するデータ量を増やしていくというプログラム的な機能拡張は、特にパブリック型のブロックチェーンでは、仕様を変えるというのは参加者の過半以上の合意を必要としますということで、簡単に仕様の変更ができないというのが論点としてございます。従ってコンピュータの性能が仮に上がったとしても、ビットコインブロックチェーンを変えようと思っても簡単に変えられないと。

今、ビットコインブロックチェーンのコミュニティに何が起こっているかというと、ビットコインブロックチェーン上に記載できるデータの量が小さいので、それを広げたいと思ってそういう意見を出している人がいるのですが、それを是とするか非とするかということで、簡単に容量、1トランザクション当たりの取引の容量を広げるということだけでも全然まとまらないという、そういうことになっています。この点がLinuxのようなオープンソースとはまた違って、完全に中央の管理者がいないために、逆に仕様の変更が利かないというブロックチェーンの弱点にもなっているというふうに考えます。

あとファイナリティ、これは決済の完了性という意味ですけれども、一般的にファイナリティは決済が無条件かつ取引不能になる、最終的に完了した状態というのを指します。しかしながら、先ほど申し上げたように、チェーンの分岐が発生し得るタイプのコンセンサスアルゴリズムですと、仕組み上、取引内容が最終的に覆る可能性が完全にゼロにはできない、ファイナリティが確保できないという弱点を持っているということです。そのため決済機能を提供する金融サービスでブロックチェーンを使うには、取引の安全性ですとか安定性、あとファイナリティの確保の観点からどう使っていくかというのは、これは論点になっていくということです。

続いて、システムの安定性、セキュリティですけれども、ブロックチェーンの利点としましては複数の参加者がそれぞれ、同一の台帳を持つということで、一部の参加者の台帳が停止したり壊れたりしても、システム全体の運行稼働に与える影響はないということです。このためブロックチェーンの技術では、一般的に実質的なゼロダウンタイムのシステムの実現ができると言われております。

「どういうときにブロックチェーンは崩壊するのですか」という質問を受けることがあるのですが、これは世界中のインターネットが全てダウンしたときということです。全てのインターネットがダウンしない限り、ブロックチェーンもダウンしないということです。ただ、当たり前なのですが、ブロックチェーン自体が止まらないということと、周辺システムですとかサービスが止まらないということは、また別でございます。ブロックチェーンは生きていたとしても、銀行の情報系とかアプリがダウンするということは、これは当然あり得ることですので、そのときに利用の可能性というのは制限されるということです。

あとブロックチェーンは改ざん耐性、不可逆性が確保しやすいという特長を持っています。このため中央の管理システムと同水準の改ざん耐性ですとか不可逆性を単純な構造で、低コストで実現

できる可能性があると言われています。ただ、改ざん耐性の水準は、今までお話ししましたように、コンセンサスアルゴリズムの影響を受けますし、業務の要件に応じて、それを満たすコンセンサスアルゴリズムの採用が必要となるということです。さらにブロックチェーン上に記載されたデータは、改ざん、取り消しができませんので、取引のトレーサビリティと透明性は向上し、例えば監査の証跡として利用できるという可能性もあります。

あとデータの秘匿性の論点ですけども、ブロックチェーンの技術は複数の参加者にそれぞれ同一の情報を共有するということで、お互いの情報を持つという前提で業務や取引がなされるものにおいてはメリットがあるということです。

一方で、そこには論点もありまして、情報共有を前提としないような業務、取引では情報管理の観点からは、取引当事者でない参加者、関係ない人も台帳記録を持つことについて法的な整理が必要ですということ。あとブロックチェーンの参加時に、どうやって情報共有しますかという容量の問題。あとブロックチェーン脱退時に情報をどうやって確実に削除しますかという、そういった論点があります。

実装時の論点として、ブロックチェーンでは複数の参加者で同じ情報を持ちますので、中央の管理のシステムと比べて、全体で見れば当事者が増えてしまうということで、銀行であれば銀行が一つのサーバーを管理すればよかったのですが、管理する人が増えるということで運用のガバナンスがブロックチェーンの場合は複雑になっていくということです。

あと改ざん耐性、変えられない、消せないといった特徴は、これはプログラムでは変更できませんので、仮に変更修正が生じた場合にどう対応するかというのは、ガバナンス上の問題になってまいります。

ブロックチェーンは、自身の関係しない取引をも記録する必要がありますので、台帳の保持に必要な情報の容量というのも問題になってきます。例えば、皆さんがお持ちのPCでも、ビットコインブロックチェーンはダウンロードして格納できるのですが、これは日々ビットコインブロックチェーンの取引が増えていくと、ご自身のサーバーの容量もどんどん食っていくということになります。

あと費用対効果の面ですが、これも非常に大きな論点ですので、これは後ほどご説明します。

今まで申し上げた一般的なブロックチェーンを金融に使う場合の論点は、ここにお示ししている９点になります。

費用対効果に対する論点についてご説明します。金融業務で使われるシステムでは、冗長性ですとか可用性の確保、改ざん耐性、トレーサビリティの確保などが重要な論点になります。これらの要件を満たすために従来の中央集権型のシステムでは、システムの多重化、バックアップをつくるなどして対応していますけども、ブロックチェーンは比較的低いコストでこういった要件を満たすことができるのではないかと言われています。そのため多くの経営者たちも含めて、ブロックチェーンの活用でシステムの抜本的な効率化が可能になるのではないかと期待されています。

ただ、コストの比較については、次の点に留意が必要だと思っています。中央の管理システムにおいて、ホストコンピュータのオープン系コンピュータへの移行、クラウド化といったコスト削減の対応というのは、もうすでに幾つかありますので、クラウド化を含めたコスト削減策との比較検討が必要です。コストの比較においては合意形成に要するコスト、あと台帳を最新に持っておくというための通信のコストというのも必要でございます。

あと、ブロックチェーンを用いて新しいシステムを作る場合はいろんな要素を勘案しながらシステム、事務の運用面を含めて全ての所有コストを明らかにして比較する必要があると。単純にサーバーを変えればよいという議論ではなくて、そこから派生して、当然いろんな業務ができておりますので、運用を変えることについての論点というのがあります。

例えば、貿易なんかでブロックチェーンに置き換えられないかというアイデアはいろいろあるのですが、事業会社の方々が行くと、もうすでに貿易については社内のシステムがありますと言われます。それを置き換えるには事後フローも変えないといけません。ですので、簡単にはブロックチェーンに置き換えるということはできませんねというようなことを言われるということでございます。

あと、IT インフラだけではなくてインフラの在り方ですとか、業務プロセスの改革によるコスト削減効果についても検討が必要になってくるという点があります。

これらの論点は、答えを持っているところはまだないと思っております。この全銀協の検討会でも、本当にコストというのは全部洗い出されているのだろうかという議論は散々しましたけども、なかなか単純に比較できるわけではないという状況です。

一方で、世の中ではブロックチェーンを使うとコストがこんなに下がるというような試算結果が、一部のコンサルの方々が出してきていますけども、それが本当なのかというのはよく考える必要があるということです。メインサーバーが要らなくなるということで、コスト削減できるのではないかと考えがちなのですが、今お話ししたような論点をちゃんと整理して、またトータルでの社会コストも含めて議論、試算することが望まれると思われます。

ここでは、今までの議論、論点踏まえまして、では金融において適する業務、不向きな業務はどこにあるのだということをお示ししております。適する業務としましては、分散型の情報連携、ビジネスプロセスの効率化、トレーサビリティの確保など、台帳を共有することでなんらかの価値観を見出せる業務とか取引があげられます。あと、リアルタイム性を求められないような業務、取引であれば適するのではないかという議論がされております。

一方、不向きな業務としましては、ミリ秒単位での高い処理性能を求められる取引、通常のシステムで対応可能な、１組織だけでクローズでやっているような業務、取引、あと単純なデータベース、ミドルウエア、トランザクション処理のシステムの代替。こういったものは逆にコストが上がってしまって、機能的にも満たされていないので不向きなのではないかと言われています。ただ、今は不向きでありましても、仕組みの工夫ですとか技術の向上で、より解決できる点も出てくると思

われます。

例えばミリ秒単位での処理速度というのは、先ほどのビットコインブロックチェーンですと10分かかるというのがあるのですが、今は技術的に10分、最終的なファイナリティはそこでかかるのですが､そこを迂回してファイナリティを仮にするというようなやり方も出てきておりますので、ここは徐々に技術的に工夫がされていくところであります。

ここからは、これまでの議論を踏まえまして、具体的な金融のユースケースに関する考察と課題でございます。

まず為替の取引です。内国為替に関しては、日本では銀行間のリアルタイム決済というのは実現しておりますので、性能的には基本的にブロックチェーン技術が優位になるというふうには考えておりません。一方で、ブロックチェーン技術では、決済システムとして不可欠な高い改ざん耐性ですとか、高可用性なシステムを低コストで実現できる可能性があると。例えば、数日決済にかかってもよいという取引であれば、安価な送金のサービスに使えるという可能性はあります。

あと外国為替取引では、銀行を介すると海外送金に数日かかるというのが現状ですので、ブロックチェーン技術の処理性能で、今までより高い性能を達成できるかもしれないということになっております。

一方で留意点、課題ですけども、実用化に向けては、これまで述べてきましたように、技術的に実現可能な性能水準、機能、あと実装やデータの秘匿性確保に関するコストを含めたトータルでの費用対効果。これらは最終的にお客様が負担する送金コストに反映されますので、どのような送金サービスをどの程度実現できるかというのがそこに影響してきます。

あと外国為替取引では、すでに商慣習とか法制度が異なる、他の国との事業者との取引になりますので、さらにさまざまな角度からの検証と合意が必要となってくるというのが論点になります。

ここで、ちょっと仮想通貨について簡単に触れておきたいと思います。ビットコインに代表される仮想通貨なのですが、日本円のような法定通貨、あとICOCAですとかPiTaPaといった電子マネー、Tポイントといったポイントとどう違うのかということで一覧にまとめております。

仮想通貨とは何かということなのですが､法律上は改正資金決済法で新しく定義されております。ただ新聞報道などでは、ブロックチェーンを使ってやりとりするようなお金のようなもの全般を仮想通貨と呼んでいるようです。ですので、新聞なんか見ていますと、法律上は仮想通貨に該当しないものも、たくさん仮想通貨というひとくくりで書かれているように思います。

仮想通貨と電子マネー、ポイントとの違いの一つとしまして、仮想通貨と呼ばれるためには、法定通貨との交換レートにボラティリティあるというところが要件となってきます。例えば、１コイン１円というように決まっているものは、これは法的な仮想通貨には該当しません。１コイン１円というものであれば、電子マネー、１コイン100円というものであればポイントというふうに法的には整理されます。従いまして、これ報道ベースではありますけどもMUFGコイン、これは１コイン１円という固定レートで決められているというのであれば、MUFGコインは仮想通貨ではな

い、これは電子マネーやポイントであるということになります。

お配りしているハンドアウトにはお付けしていないのですが、私ども三井住友銀行のほうで行った、ブロックチェーンを用いてつくった仮想通貨、今申し上げたように法的には仮想通貨にはなりませんので、ここではデジタル通貨と言いますけども、その実験の内容をご紹介します。

私どもの部内で、ブロックチェーン上でつくられたデジタル通貨、これは部内でマロンコインと呼んでいるのですが、それをつくっております。中身としてはMUFGコインと同等のものというふうにお考えいただければと思います。そのマロンコインを実際の店舗の物品購入に使うという実証実験を行っています。

デバイスは、写真見ていただけると分かりますように、利用者側、店舗側、いずれもNFC対応のスマートフォンを使っております。つくったマロンコインをスマートフォン上のアプリにまずチャージしています。今回、1マロンコイン1円でやりました。当社の社内の売店で、例えば600円の雑誌を購入します。そのときにはチャージされたスマートフォンを店舗側のスマートフォンにかざして店舗側にマロンコインを支払います。支払いが完了すると利用者側のスマホの画面上で使われた600円のマロンコインがチャージから引き落とされるということです。マロンコインを受け取った店舗側は、マロンコインの発行者、この場合は私どもの部になりますけども、こちらから600マロンコイン相当の円、600円を受け取るという、このような実験を行いました。

デジタル通貨をつくって実際に使ってみての感想なのですが、Suica、PASMOをかざして物を買うときと何らかの変わりがないということで、確かに裏ではブロックチェーン上に取引履歴、残高記録が記帳されているのは別に確認はできるのですが、インターフェース上はブロックチェーンを何らかの意識することはありません。

この実験で分かったことは、価値の移転ということに関しては、デジタル通貨と電子マネー、ポイントというのはユーザビリティの観点では何らかの変わらないということです。「電子マネーと何が違うの」というのは、率直な感想です。

そう考えますと、ブロックチェーンのユースケースとしては、単純な価値、移転に注目すると、すでに電子マネーですとかポイントという代替物が存在しているということになります。であれば、もっとブロックチェーンの固有の機能、改ざんできないですとか消せないといった機能に、よりフォーカスしたユースケースを考えたほうがいいのではないかというようなインサイトが得られた実験でありました。

ここではあまり踏み込みませんけども、ビットコインのような仮想通貨、国が発行するデジタル通貨、銀行が発行するデジタル通貨、あとベンチャー企業が発行するデジタル通貨、これいずれもつくり出すことは可能なのですが、ブロックチェーン上に記載される価値ではありますけども、では誰が発行した、あるいは誰が価値を裏付けるマネーを信用しますかという議論になっていくのかなと思います。これは仮想通貨とデジタル通貨、加えて法定通貨との関係ということになろうかと思いますけども、ここでは問題提起にとどめておきます。

次のユースケースとしてKYC（know your customer)、本人確認についてご紹介します。現在KYCは各銀行がそれぞれ行っていまして、莫大な事務コストが発生しているということです。銀行ごとに手続きが異なりますので、お客様に手続きの負担が生じているということもあります。このKYCにブロックチェーンの情報の共有、高い改ざん耐性という特長を生かして、銀行の壁を越えたタイムリーで正確な情報共有ができないかということです。情報のバックアップの観点からもブロックチェーンによって分散管理が実現できれば、ハードウエア設備のコスト削減にもつながるのではないかというふうに言われております。

一方で、留意点、課題ですけども、KYCの情報は他のユースケースと比べましても個人情報でありますので一般的に高い情報の秘匿性が要求されます。セキュリティ対策を含めてこれに応える技術が必要となると。プライベート型、コンソーシアム型、いずれにおいても法的な論点が必要になってまいります。個人情報の取り扱いに関する責任所在の明確化、参加者間の責任分界、問題解決方法のルール化といった論点がありますので、それぞれの関連法令に基づいて検討が必要であるということです。

今、実務者として大きく感じていますのは、現時点でブロックチェーンの活用のボトルネックとして何があるかというと、技術活用の広がりに法的な整理が追い付いていないという点です。また後ほど久保田先生から詳しいご説明あるかと思うのですが、価値移転ですとか債権債務の関係に関して言いますと、司法上、公法上、ブロックチェーンの記帳上の価値移転と法的な価値移転が一緒になっているのかという問題もあります。あとファイナリティまでの時間10分間、債権債務はどのように扱われるかといった点も、まだクリアではないということで、こうした法的な整理が進まないと、特に金融のところではブロックチェーンの利用に及び腰しにならざるを得ない。ブロックチェーンを巡る法的理論の整理が待たれるというふうに感じております。

実際にブロックチェーンには、いろんな特徴がありまして、価値はどんどん移転していくのですが、ブロックチェーンというのは、価値が移転していくだけのものですので消せません。その場合に何が起きるかというと、債権債務という貸方借方の考え方がブロックチェーン上にはないというのが実験で気付きまして、債務を消すというのは、実はブロックチェーン上はできないのではないかというのが最初の実験で気付いたことで、これはなかなか、技術的には可能になっても、法的にはそれは可能だけども技術的には消せないということをどうするかというのが、最初の実験したときに出てきた論点でありました。これ法的な論点にもなりますので、また議論できればと思っています。

あと勘定系システムでの利用です。銀行の中核システムを処理する勘定系システムですけども、高い信頼性と安定性が求められるということで、ブロックチェーンの特長、ゼロダウンタイムなんかが実現できればバックアップが要らないといったコストメリットが生まれる可能性があります。プライベート型を採用した場合は、運用ガバナンスはある程度自分でコントロールできる可能性があるので、導入に伴う影響が少ない可能性はあります。

あと、ここに書いてないですけども、スマートコントラクトと、更新系の金融の API、API は今、金融でも非常に話題というか大きなテーマになっているのですが、API が繋がりますと、例えば、顧客の企業が売買契約に基づき入金や出金をする操作というのは、金融機関に対する入金出金の指示を経ることなく共有されて、スマートコントラクトに基づいて入出金がされるというような世界が来るかもしれないということです。

ただ、金融の勘定系の既存システムにブロックチェーンを適応する場合、高いセキュリティが求められるということです。住信 SBI ネット銀行が勘定系のブロックチェーンを使った実験をしましたが、ネット銀行の強みである軽い勘定系だったからできたという面もあろうかと思っております。勘定系のシステムは、またシステムの中心的な機能となりますので、ブロックチェーンを使う場合、先ほどの勘定系とアプリの関係ですけども、情報系をはじめとする周辺システムとの接続についても検証することが必要ということになってきます。

このように、ブロックチェーンを既存のレガシーな巨大システムと置き換えるには、まだまだ課題があるというふうに感じております。ちょっと時間の関係で金融インフラのところは割愛させていただきます。

最後に、私が考えるブロックチェーンと金融の今後の展開、ブロックチェーンの今後について一言申し上げますと、この後も登壇される先生方、パネルディスカッションでいろんな意見が出ると思いますので、金融という観点から申し上げますと、ブロックチェーンは金融と親和性が高いのではないかという仮説の下で、金融分野でユースケースの開拓、検証が先行していたという面はあると思います。ただ数年前から金融分野のブロックチェーンに携わっていたものとしては、ブロックチェーンというのは金融だけではなくて、その他の非金融分野、むしろそちらのほうがフィットするのではないかというふうに思っています。特に、真正な台帳の必要性ということでは公的サービスでの利用がフィットするのではないかと思います。

あと足元の技術の進展を見ますと、非金融分野でのスマートコントラクトの活用の可能性があると思っています。スマートコントラクトのインパクトを一言で言いますと、デジタルとリアルなものが結び付く世界が来るということだと思っています。例えば、レンタカー契約がスマートコントラクトに乗せられて、スマートコントラクトで契約指示をキックに車というものが動くということが実現されます。デジタルの世界で OK が出なければ車が動かないという世界が来るということです。

こうしたブロックチェーンを取り入れたデジタルの世界というのが広がるということは、金融機関にとっては非常にいいことだなと思っていまして、もともとデジタルの世界に親和性のある金融ですので、マネーと物が一体化していく世界が来ると。そのきっかけがブロックチェーンなのではないかというふうに考えています。

私からは以上です。ご清聴ありがとうございました。

講演 3

「個人情報の有効活用を可能にするブロックチェーンの考察」

産業技術総合研究所　情報技術研究部門　宝木　和夫

産総研の宝木です。

本日は、文系の講演会でお話しするというのは初めてでして、暗号のような非常に数学がベースの技術をちゃんとお伝えできるのかどうか、いささか自信がございません。ですが、できるだけ数学というものを国語的に紹介するようにしたいと思っております。本日の内容をある程度ご存じの方は、退屈な内容かもしれないですが、最新のテクニックもご紹介していますので、ご容赦ください。

まず、スマートコントラクトという文脈から、少し情報技術の進展のタイムアラウンドを見たいと思います。スマートコントラクトという概念が、初めて提示されたのが 1997 年、ちょうど 20 年前です。現在、情報技術はようやく実用化されて、スマートコントラクトがようやくビジネスで実用化されて来ている。やはり情報技術の分野は、理論が出ても世の中に普及するにやはり 10 年では足りない。20 年ぐらい見ておくという必要があると、そういう感覚であると思っております。

このスライドの通り、最初の発想はすでに現在の問題をかなり言い当てていると思っています。つまり、スマートコントラクトというものは、プロトコルとユーザーインターフェースを組み合わせ、コンピュータネットワーク上の関係を形式的に表現し、セキュリティを確保するということです。この言葉が出て来たときに、われわれ暗号の研究者、セキュリティの研究者というのは、「ああ、いよいよわれわれが期待されているかな」と、元気づけられた論文であるわけです。特に、暗号その他技術の利用や、機関、ユーザーインターフェース、アルゴリズム技術の安全性は重要であるというところです。

この観点が出た情報技術の背景というのを見てみますと、ポストモダンという、コンピュータができた故に世の中の人々の考えが変わった時期に対応して、メインフレーム以降いろいろ技術が出てきました。スマートコントラクトが出た頃は、インターネットが始まって、関連する認証暗号技術がようやく使われだした頃でありました。

それからしばらくして、ビットコインなるものが 2009 年に出ている。まだ 2009 年でしたので、ここから 10 年、20 年とかけて成熟していく可能性が高いと思っています。その意味で、まだまだ情報技術的には、実用化という面ではまだ油断できない、柔らかい技術であると認識したほうがいいと思います。

ビットコインが、地球にある金塊のような働きを仮想的に実現しているというのは、本日の講演で佐々木先生はじめ先生方が、言われていたとおりであります。ビットコインは、実際は、コストをかけて採掘すれば自分のものになるという金塊の概念です。そして、その埋蔵量は有限であります。それを情報技術でどのようにやっているかといいますと、各人は公開鍵の名札付きの財布にビットコインを入れるということです。公開鍵というのは、暗号で秘密鍵と公開鍵がありまして、秘密鍵は自分だけが持つという暗号であり、公開鍵は皆に公開するという暗号である。自分で署名したものは、皆が公開鍵で確認することができる。皆が公開鍵で暗号化すると自分だけが解けるというペアの関係になっているものです。そして、公開鍵が付いた、名札が付いた財布、公開台帳があって、そこにビットコインを入れるわけです。

つまり、公開鍵というのは、ビットコインを入れるアドレスとして使われるということです。公開鍵は、各人が勝手に生成していいというところがポイントです。ここに中央機関は存在せず、自分で作って公開するということです。一方、秘密鍵は、各自が大事に保管するというところです。これが最初の始まりで、数学を使わずに、非常にシンプルかつ国語的です。

システムの仕掛けですが、プルーフ・オブ・ワークというものがあります。いわゆる金塊を掘る採掘者（マイナー）が必要です。このスライドにあるように一生懸命努力して、実際にはコンピュータの計算力を使って、最も早く金を見つけた人が受け取るという感じです。最も早く問題が解けた人が、報酬として金を最初に受け取ることができる。公開台帳については、ブロックチェーンの正当性をチェックするための作業台がそれに当たります。計算量が必要ということで、その採掘作業が計算量の証明、プルーフ・オブ・ワークといわれています。

台帳のイメージはこのスライドの通りでして、例えば、公開鍵とつながっているアキコさんの財布には、先月より５月１日に繰り越されて 35 万円入っています。ここで、イチロウさんへ１万円を送金すると、アキコさんの残高が 34 万になったとします。そうすると、イチロウさんの財布は、50 万から 51 万に増えることになり、科目のところ、摘要のところに送信者と受信者の名前が入ります。もちろんここでの名前は、中央集権なしに勝手につくる仮の名前で大丈夫です。これで、なぜお金が移ったことにしていいのかというのが、マイナーの仕事となります。

このスライドが処理を示しています。現在の状態では、公開鍵 P_A、つまり、アキコさんの公開鍵が書いてあるこの台帳に 35 万円が入っている。そして、公開鍵 P_B というレッテルが貼っているイチロウさんの公開鍵に１万円を送金し、残金は 34 万ですというメッセージを秘密鍵 S_A として、アキコさんの秘密鍵で署名して公開する。これで、送信者の処理は終わりです。あとは、台帳に記載されたＡに 34 万、Ｂに 51 万が存在するというのをマイナーが認めるということです。本当ならば、全員が認めて多数決で投票すればいいのですが、それは大変なので、１人が代表して頑張って行います。ただ、簡単にできてしまうと、金塊としての価値がなくなってしまうので、努力が必要となる。

実際にはどういうことをやっているかというと、マイナーをＣさんとしてお話します。公開され

た署名を見まして、アキコさんから１万円減ってイチロウさんに１万円増えているという状態１の帳尻が合うかを見ます。そのメッセージに加えて、あとは過去の履歴です。それをメッセージ上でつなげて、それをここではＭと書いています。ラージＭ、履歴とそのときのトランザクションです。それに、とりあえず乱数を生成してくっつけます。それでハッシュ関数を取ります。そうすると、最初のハッシュ値は、最初の１ビット目、０と１になる確率は、0.5 です。これを、何回もやります。最終的には、０、０とか、何回もやると、たまたま出てきます。この０が多ければ多いほど、２の冪乗計算量が増えますので、それだけ試します。例えば、最初に０が何十個か決められた値になるような、Ｒを一番はじめに見つけたら、それでマイナーは成功する。そのＲを使って秘密鍵で署名するということです。これは、皆が確認することができます。マイナーの公開鍵で、お金を入れていいよということで、自動的に例えば１ビットコイン、今なら１回当たり 100 万ぐらいもらえるというです。ただし、もらえるのは１番目だけです。

これを図で描くと、スライドの通りです。ここでは、以前の発掘者から今回の発掘者の処理の移転を示しています。マイナーはその都度やっていくのですが、数字はもうちょっとトランザクションがたまってからやる。たまるまでもっと早くしてくれと言ったら、マイナーにたくさん払えばやってくれます。

状態には、Ａに 34 万、Ｂに 51 万と、それぞれアキコさんとイチロウさんに存在する。それでマイナーであるＣに、本当は実際にはもうちょっと多いですが、１ビットコインが入る。それが確認済みの状態になって、Ｃには規約によって採掘料が入る。あるいは、Ａがちょっと急いでいるなら、もうちょっと多めにチップをはずんでいるということもあります。その後、別のマイナー候補が同じように別のＲを見つけたとしても、２番手はもらえません。これを繰り返すということなので、いわゆる簡単明瞭だと思います。

あと、上位レイヤのプロトコルという規約があります。発掘に見合う発掘報酬というのは、ビットコイン累積発行量が増えると、暫時減少するという規定になっていまして、２万 1,000 ビットコインが累積発行された時点で発掘報酬はゼロになります。それ以降は、実際に送金者が色を付けて、「これだけ何ビットあげるからマイナーして」と言うことが必要になると思います。

金融庁が仮想通貨を貨幣認定したのは 2016 年２月で、本当に最近です。代表的な仮想通貨はビットコインですが、その時価総額は去年の１月時点で１兆円で、実体経済に影響を与えるほどではない。しかし、おそらくこれが３桁ぐらい多いと、絶対に当局が出てきます。まだ１兆円だから、普通の電子キャッシュと一緒の扱いとされています。

ただ、注意すべき点は、ビットコインは認証方式として楕円曲線暗号を採用していますので、量子計算機がいつか出来たときは、この仕組みは崩壊します。ただ、直ちに累積データが全部改ざんされまくるとは非常に考えにくいです。ハッシュでのチェーンになっていますからとても大変です。過去の取引の証拠はあちこちに残ります。しかし、暗号が破られた後の取引は証拠性がなくなります。したがって、ある日、量子計算機が成功しだしたというニュースが出たら、ビットコインは暴

落しますので注意が必要だと思います。

ビットコインの課題でございますが、このアキコさんの公開鍵、イチロウさんの公開鍵というのは、必ずしも実名につながらなくて、勝手に作って公開した仮名でよいものです。中央機関がないので証明をしようがないです。ただし、同一の仮名を使って取引を続けていますと、統計的推論等によって実名および取引関係等が割り出される危険が増えます。これは、リンク可能性といいます。仮名間での通貨のやりとりは、大丈夫と思うかもしれないですが、オープンデータに残されたこの履歴は、未来永劫残ります。将来、AIによっていつ割り出されるかもしれないという恐怖感はあります。仮名であっても、それ以外の別途のショッピング履歴とか、いろんな履歴を見ると、銀行口座からの引き出し履歴とか、それらが残っているというのは、やっぱり非常に気持ち悪い感じがします。

先ほどのレガシーの金融だったら別にどうっていうことはないのですけども、そうでない方々もいらっしゃいます。そういう方には、やはり気持ち悪いということで、このリンク可能性を避けるためにビットコイン利用者の多くが行うのは、仮名、つまり公開鍵を頻繁に変えている。あるいは、分散したり迂回経路を用いるなど、種々の工夫をしていると言われています。ただし、どれぐらいなのかについての統計データは出ていません。

結局、マイナーのお仕事は増えていいのですが、いわゆる支払料金の増大とか、あるいはそのための無駄な労力、人件費とか、そのためにコンピュータを動かしていますから、コンピュータの電気代とかがかなり増えます。もちろん、世界中で広くてやられているだけで、絶対量としてはまだ大したことはないと思います。

やはり一番の課題は、こういう値段や電力というよりも、匿名性についてです。一般の人にばれる確率はあるし、当局者にもばれる確率はあるということで、やはり匿名性がはっきりしないということです。

とうことで、これからさらに一歩ずつ進んで、匿名化を強化する実際の手法をご紹介したいと思います。アキコさんから第三者機関にまず１万円を送る。プール預金ということです。その後、第三者機関が、イチロウさんに事前にアカウントと暗証番号を教えます。これによって、イチロウさんは、アキコの預金を引き出せるようになります。ただし、ここで要求されるのが、第三者がリンクをしないというリンクの不能性の保証であります。あとは、第三者機関の処理の透明性というものが必要となります。あまり分からずにとにかく信頼してやるという信頼モデルもありますが、ここでの実現モデルの理想としては、透明性が欲しいということです。

これを実現する方式が発表されています。その前に、ゼロ知識証明を、数式というよりも国語的にご紹介させてください。hというのは、ある性質を持つ関数であります。計算式ですと、$y=h(x)$なるxを知っていることを証明するということです。例えば、デジタル署名をイメージしてください。yが署名後のメッセージであるとすると、これをもらった人は、相手はこういう計算式を導く秘密鍵を持っていると納得しますので、デジタル証明の仕掛けが動いています。ただ、いわゆる

ゼロ知識証明は、もうちょっと広くテキストを表現できる能力がございます。少なくとも、このｘを示さずに証明を行いますので、基本はｙとｈを教えることになります。これは、公開鍵の情報も含まれます。一つの例は、デジタル署名の確認なのですが、一般的な表現でいうと、秘密情報を知っているということを証明してしまおうということです。さらに国語的に表現すれば、長編の小説で、犯人の名前がずっと分からない状態であって、犯人を明かさずに「俺は犯人を知っているんだ」と証明するようなものです。

さらに、チャレンジレスポンスというのを使わずに、事前に証明値ｚを計算して相手に送ることもあります。これは、デジタル署名そのものに近いです。少なくともこの情報の出元は分からないが、これを満たすｘを知っているということは納得でき、それが証明となって実際のお金が移動するというバイタルな情報になっている。ただし、デジタル署名と違って、この表現能力は非常に高いです。現状、ｈの性質というのは、結構限定されています。将来、もう少し情報研究が進むと、かなり自由な表現ができるということが、原理的には分かっています。

ゼロコインが出たのが、ほんの４年前です。これは、これから 10 年、20 年かけて、おそらく世の中に浸透するかもしれない。あるいは、これは似た概念ですね。ゼロコインでは、第三者機関のところが公開台帳に替わっています。非常に不思議な感じですが、これでできてしまいます。

ここで、アキコさんは「コインの移動」を行います。この式ですね、f(g(7386276), x) = 27349209 を満たす値を知っているということです。それのゼロ知識証明を付与するということですが、明らかにするのは 27349209 という値で公開台帳に書く値はこれだけです。この式を満たす、二つの数値、7386276 とｘが暗証番号になります。これを、イチロウさんに教えてしまう。ここでは、１回のコイン移動で１万円が行くという規約としています。

その後、引き出しという処理があります。イチロウが引き出すときは、暗証番号をマイナー、あるいは皆に見せる。これはどういうことを証明するかというと、あるｘとどれかの登録番号が、どれかでこうなるような数値を知っているということを証明します。つまり、ｘとｚのゼロ知識です。ｚというのは、この預金者の登録番号で、これらを組みとして明かさずに知っていることを示すということですね。これによって、マイナーは、このイチロウさんに１万円移ったということで証明するという形になります。このとき、ブラックリストには、この 7386276 を載せていますので、２回目に知らせても、２度払いはできませんというふうになっています。

これがゼロコインでして、その変化形はいろいろあって、もうちょっと金額がバリエーションできるとかいろいろあるのですけれども、ある前提下では、安全であることが証明されております。

また、ゼロコインの拡張ということで、ゼロコインは非常に匿名性が高いです。仮名間でも、リンクを切ってしまうので、匿名性という意味では、非常に健全な仕掛けです。一般に対して変にプライバシーがばれないだけでなく、当局者にもばれないです。それはちょっとまずいんじゃないかということで、せめてオンブズマンとか監査者を選んで、いざというときは監査者がせめて仮名間でリンクできるようにしたいというニーズがある。

ということで、追加処理は、これもちょっと付ける感じなんですけども、アキコさんの処理をやっているところの中間値 g(7386276)、この値に対して監査者が解ける形のエルガマル（ElGamal）暗号を生成して載せる。それは、この 66489207 という値になります。これはいわゆる確率暗号といいまして、一つのメッセージに対して暗号文が大量にあります。誰か別の人が同じように暗号しても、別の字面の暗号文になるという性質のものです。

これをやる場合にも、やはりゼロ知識証明を付けておきます。ただし、証明値を一緒に載っけないといけないという規約に変えないといけません。マイナーはそれを確認して、お金の移動を完了させます。これで、イチロウさんの処理は、従来と変わりありません。ただ、この監査番号が残っていますので、監査者はいつもアキコさんの口座からイチロウさんの口座へ移ったということは、この暗号の突き合わせをやることでできる。アキコさんが入力した 66489207 を復号化した数値と、イチロウさんが入力した 7386276 を関数 g で変換した数値が一致すれば、それらはつながっているということになります。これも一応ゼロ知識証明のリレーでやっているので、監査者以外にはリンクできないということは証明されます。非常に閉じられた前提ですけども、数学の世界では証明されていると。

数学の証明というのは、ご存じのように、神様の証明と一緒で皆さん信じています。これは非常に説得力があります。ただ、これを実現する周辺のいろんな柔らかい情報技術がありますから、そこはいろいろ問題がでてきます。ここでは少なくとも、ここについては数学という圧倒的説得力のある信用の証明が付くということです。やはり、これも電子現金、送金に値するそういう信用を持たせるためには重要なところであろうというふうに考えております。

監査機能の意義ですけども、オープン環境、仮名と送受信者間のリンクを断ち切る機能を入れたデータ送受信の仕組みで意義があると言えると思います。ゼロコインという仕掛けは、安全かつ個人情報が守られる度合いは高いです。少なくとも、ある閉じた狭い部分では証明済みです。しかし、監査は困難ということで、データ送受信に関して一種の無政府状態になるという危惧がございます。監査機能付きの仮名データ送受信の仕組みというのは、一種の無政府状態のデータ送受信をよしとしないアプリケーションに向いています。

ということで、別途、法令遵守が義務付けられている個人情報保護のアプリケーションでは、監査機能は明らかに有用です。むしろこういう監査機能は、むしろ匿名現金以外のエリアではっきり有用性があるのでないかということで考えております。

この個人情報の二次利用の応用について、少しだけお話させていただきます。例えば、何か災害が起きたときに、システム適応能力が問題となります。特に大きな問題になったのは、東日本大震災のときです。ライフラインのほとんどは寸断されましたが、通信網は比較的早く戻りました。そこで何が問題になったかというと、移動や移送ロジスティックの応急処置、回復に必要な情報がうまく使えなかったということです。

例えば、自動車、人の位置情報が取れないということで、避難指示が有効活用できなかった。そ

れから、医療情報や生体認証情報が取れないということで、避難所のケアに支障があって、そのために市役所の職員の疲弊につながっているという側面もありました。本来、活用することができれば有効なはずの情報が、プライバシー保護やセキュリティの壁に阻まれ活用できないということで、被害の拡大、復興の遅延を生じさせてしまった。これは極端な例ですが、個人情報の二次利用を考えることには意味があると考えております。

基本的には、個人情報の二次利用を許した途端に、個人情報について自身のコントロールが利かなくなりますので、大きな問題となります。そのため、基本的にはその個人情報の移動の履歴を取る、かつ監査可能にするというところです。

さらに、ブロックチェーンと監査機能とを入れるときに、誰が監査をやるのかということです。データコントローラというのをしっかり決めて、情報の二次利用に関する認証をタイムリーに与えるようにすることなどが必要となります。

もう一つは、上位の仕掛けですね。サーバー系の管理系、特に、SOX 法なんかで実現されています組織内の厳重なアクセス管理です。そういうコンピュータを持ったところで個人情報というのを扱う仕掛けが必要になる。たとえカルテの情報そのものを厳重に管理しても、それを見た人が、例えば「この人は余命何年のがんです」と言うと、それは個人情報の漏洩になります。それを防ぐ仕掛けがやはりインサイダー取引を防ぐのに現実に役立っているようなアクセス管理の仕掛けとか、コンピュータ内部の監査の仕掛け、そういうのを含めて実現するということが必要になるかと考えております。

最後に、健全性とか完結性などのエラーはあるが、とにかく緊急時に個人情報の二次利用をできる仕掛けについて、ブロックチェーンとかゼロ知識というのは有効ではないかという仮説についてお話させていただきました。以上で終わりたいと思います。どうもありがとございました。

第二部：
ブロックチェーンの
法的・経済学的論点

講演４

「ブロックチェーンの法的課題」

早稲田大学法務研究科　教授　**久保田　隆**

ただいまご紹介に預かりました法務研究科法学部の久保田隆と申します。今回はこのような貴重な機会を与えていただきましてありがとうございます。

私は法的な課題をご説明するのですが、実は法律というのは、皆さんが思うほど、これは丸です、これはバツですと議論を固定化してしまうものばかりではありません。むしろ将来に向けてオープンな議論を開くものです。

例えば、先ほど三井住友銀行の竹田さんのご報告でMUFGコインは、１コインを１円に固定しているため資金決済法上は仮想通貨には該当せず、通貨建て資産、すなわち電子マネーであるとのご説明がありました。これは確かに現時点の法解釈としては正しいです。他方で、MUFGコインは仮想通貨を念頭に開発されたものなので仮想通貨と同列に議論することは当然重要であり、仮に現在の法的位置づけが仮想通貨ではないから仮想通貨として議論してはいけないとまで主張するとすれば間違いです。一部の弁護士に多いのですが、法的な議論の中で仮想通貨とMUFGコインを並列に扱ったら間違いだとして、議論そのものを得意気に門前払いしたがる方がいます。しかし、彼らは法律家としては決して優秀とは言えません。なぜならば、電子商取引やブロックチェーンの法分野では、「技術中立性」（法律が将来の技術発展を阻害しないようにすること）の尊重が世界の常識であり、MUFGコインや類似のコインの今後の発展次第では、資金決済法の仮想通貨の定義に含める改正は今後十分あり得るものであり、経営者を相手に法的アドバイスをするならば、将来の改正まで踏まえた議論をしなければ何の役にも立たないからです。

また、一般論として、法律問題はTVの法律相談番組のように単純明快に法的な答えが１つに決まるケースはむしろ少なく、様々な解釈に基づく複数の答えが併存し、その中で討論されます。Ａが正しいって言った人も正しい、Ｂが正しいって言った人も正しいとした上でＡかＢかを論争するとなると、法律家ではない皆さんは混乱すると思います。しかし、法律とは本来そういうものです。私がこれからするお話は、そういう法律の性格を前提とした上で、基本に立ち返って法律上何が問題になるかということを考えていきたいと思います。

最初に、前提認識と現状についてお話しします。前提認識というのは、今まで中央管理型と分散型のブロックチェーンとで、どう違うのかが肝になります。

ブロックチェーン取引になると何が良いかというと、暗号技術の組み合わせでセキュリティが確保できるということです。それにより、サービスの利用料金を引き下げられる。そうすると、今ま

でセキュリティに問題があって進まなかったクラウドが徹底活用できるとか、あるいはモバイルＰ２Ｐの徹底活用が可能になる。総じて言うと、普通のパソコンやスマホ、ネットでも銀行と同じことができるんだったら、今ある銀行業に大きな変革をもたらすかもしれない。現在は、先ほどのMUFGコインができたり、住友銀行のマロンコインが開発されるなど、各社が様々にビジネス発展を模索している段階であります。

そこで、法的にどういうことを考えるべきなのかというと、将来的な法的対応まで見通す必要があるように思います。普通の法律家は、例えば業界団体から報告書を書いてくれと言われれば、それに対して都合のいい報告書を書くことが仕事です。一方、私の仕事は早稲田大学法学部の教員なので、ブロックチェーンの影の部分や法律家としてはもしかすると耳が痛いようなことも考えてみたいと思います。

現在の中央管理型が分散型、すなわちブロックチェーンに代わる。そうすると、例えば加害者の特定が困難な場合も出てきます。例えば、犯罪が人工知能によってなされるかもしれない。ところが人工知能は、法的には被告になれません。「こいつを裁きましょう」と言っても、裁判所でコンピュータを裁くわけにはいかないのです。そうすると誰を被告にするのかという問題が出てくる。プログラム設計者なのか、あるいは裏で操作した個人なのか、そもそも裏で操作した個人って簡単に見つかるのかと、こういう問題が出てきます。

また、今はまだ草創期ですからあまり現実味がないかもしれませんが、例えば、Google、Amazon、Appleなど情報インフラの決済サービス（プラットフォーマー）がブロックチェーン化して巨大化すると、寡占化、独占化という問題が出てくる。後で述べるように、これまで決済を寡占・独占してきた銀行業界にも大変革をもたらしますが、どう対処するかという法的な問題があります。

次に、新技術への法的対応の仕組みの問題があります。ブロックチェーン上の資産について、国家が押収するとか、差押えるとか、従来可能であったことができるのかという問題であります。もし仮想通貨しか財産がないような場合、仮想通貨は取消や巻戻しが困難なので、どうなるのか。ハードフォーク等を介して仮にできた場合でも、他の参加者の財産にも当然影響してきますので、その人たちが合意していないのに勝手に財産を取り上げられるのか、あるいは国家が暗号処理されているものに対して暗号キーを必要に応じて入手できるのか、といった問題が想定されます。

もう一つは国際化です。 先ほどApple Payの話をしましたが、もしそれがブロックチェーンとして寡占化すると、容易に国際化します。仮にそこで他人のお金をだまし取るなどの不法行為が起きた場合に、どこの国の誰が裁くのか。もちろん、法律上は不法行為地で裁くとなっているのですが、こういった分散型ですと、不法行為に関与したノードとなるコンピュータは各地に存在するわけです。そうすると世界各地で裁判が始まる「並行訴訟」となり、各地で各々判決がだされます。しかし、その判決がそれぞれ相互に矛盾していた場合でも、各々が主権国家ですので、これを調整する手立ては乏しく、従来よりも並行訴訟に伴う困難さが生じやすくなると考えられます。

さらに、裁判とは別に行政、すなわち、国際規制管轄の問題も生じるでしょう。個人情報保護、マネロン、独禁法などは、特にアメリカとかヨーロッパが、自分の国を超えて自分の国の影響を及ぼすことになる。例えば、日本企業に対してアメリカ法やEU法を適用し、高額の罰金を科すということがよくあります。これに加えて、もともとサイバー空間に対する法の域外適用は、物理的空間に対する法の適用に比べて明確な規制が乏しく、域外適用し易い性格があります。例えば、アメリカが海外に刑事を送り込んで捜査するのは主権侵害であり、相手国の許可がない限り実際にも困難ですが、海外のコンピュータにスパイウェアをしかけて容疑者情報を入手するのは主権侵害ではありますが、相手国の許可なく行うことが現実に行われており、サイバー空間は域外空間と必ずしも認識されていないためこれを規制することは法的に困難です。サーバー空間であるブロックチェーンについては、それが国際化すると、当然そういう域外適用の問題が起こり得ます。この域外適用については今のところ法律的に完全な国際法による解決策はありません。

もう一つ別の角度からいくと、このAppleのようなプラットフォーマーといわれる情報インフラサービスと銀行業が将来的に対決する可能性があります。プラットフォーマーに対する規制は現在殆どありませんが、銀行は昔からがんじがらめの規制を受けてきました。これは、銀行が決済システムをほぼ独占した状態にあったからです。しかし、この前提が変わるとどうなるか。プラットフォーマーに規制を導入するのか、あるいは銀行が他事業へ参入できるよう規制を緩和するのか。例えば、最近の資金決済法改正では、アメリカに倣って、銀行がIT企業に出資できるようになりました。他方、アメリカでは、このプラットフォーマーに対して情報インフラ提供責任とか、いろんな方面からも規制導入論がありますが、こうした点も考えていく必要がありそうです。一方、銀行による決済システムが縮小すると、当然、各国の通貨（法貨）にも影響が及びます。すなわち、仮想通貨の利便性が高まると、法貨を駆逐し、国家の通貨発行権が脅かされます。従って、各国政府は現在、仮想通貨の技術を応用した法貨、すなわち「デジタル法貨」（例：デジタル円）の研究開発を進めており、イギリス、カナダ、シンガポールが積極的です。情報をあまりオープンにしたがらない日本銀行でも実は継続的な研究を続けています。

最後に、国家規制からの独立について考えてみましょう。DAOというドイツの仮想通貨の運営会社では、自分たちはいかなる国の規制にも裁判管轄にも服さないという立場をとっています。すなわち、自分たちが書き上げたコンピュータプログラムであるコードだけに縛られる、The code is law. と主張しています。ただ、これを認めてしまうと、各国の伝統的な司法制度や金融制度から逸脱することになり、容認できません。このような問題が将来的にはありますが、以下では近未来における検討項目を考えみたいと思います。

まず、契約、すなわち民間対民間で問題となる私法上の論点です。民法の原則でいきますと、ブロックチェーン取引は今まで何度もほかの方の説明がありましたように、即座に取引が確定しない（例えば、ビットコインは10分かかる）上、一旦確定すると、今度は取消や巻戻しができません。従って、例えば、スマートコントラクトで動いたAさんからBさんに対する資金について、ブロック

チェーン以外の通常の取引と同様に、ＡさんからＢさんに対する債権譲渡と直ちに法律行為に結び付けることができず、その後、取消が生じた場合に実際に取り戻すことも困難です。従って、ブロックチェーン取引による資金移動は単なる証拠であり、法律上の抗弁にはならず、契約書で別途、法律関係を規定する必要があります。

また、金融取引では相殺やネッティングと呼ばれる相殺類似の取引がありますが、相殺では倒産時に管財人の否認権行使の形で取消や巻戻しが起こるので、やはり法律行為と帳簿管理とを別に考える必要があり、契約書で法律関係を明確にしておく必要があります。一方で、やや厄介なのは第三者との関係です。いくら契約書で法律関係を規定しても、契約当事者ではない第三者、例えば会社が倒産した場合に立つ管財人など、との関係は規律できません。では、第三者との関係が規律できないので、ブロックチェーン取引はやめた方が良いのか？

この問いに対する私の答え結論は、「細かいことに過度にこだわるな」ということです。倒産等の発生確率は低く、発生した場合も担保等である程度リスクをカバーできるし、通常であれば契約書で法律関係を規律できます。これから大いに発展可能性のあるブロックチェーン取引について、倒産時に問題が生じ得るから止めろという法律家も多いでしょう。しかし、法律家の役割はビジネスのサポートです。草創期においては、万が一の可能性はある程度無視するか、あるいは保険金とか担保とかである程度リスクをカバーできるのだから、法律家は出来ない理由をとやかく並べるのではなく、ビジネスマインドを持って契約書を最大限工夫すべきと考えています。例えば、ある取引について法律意見書を求めると、法律家、特に若い弁護士は、「いや、こういう可能性もある、ああいう可能性もある、ここが違法な可能性もある」と言って、担保等でカバーできるものや発生確率が低いものも含めていっぱい書き込むわけです。そうすると、皆さんがビジネスをやりにくくなります。しかし、収益性の高いビジネスに入るときには、白と黒の中間のグレーのところに入っていくことが大半です。従って、成長性の高いビジネス・チャンスに対しては、あまり法律的にきつく考えすぎても駄目で、ビジネスマインドの中で判断するしかないと思います。

登記・登録について簡単にご説明します。登記や登録をブロックチェーンで行うことは可能か否かという議論があります。不可能とする議論もありますが、レジュメでは可能とする立場の考え方を紹介しています。すなわち、もともと登記・登録という制度は、登記・登録があれば真実性、すなわち本当にその権利を持っていること、を推定するわけではなく、単に公示するものにすぎません。従って、これはブロックチェーンに載せても問題ないだろうという考え方であります。

一方、預金通貨に用いる場合についてはビットコインの場合にいろいろと難しい問題があるのですが、レジュメの中で触れた「ハードフォーク」について、少し説明したいと思います。

ハードフォークというのは、該当仮想通貨のルールを変える際に旧ルールを無視し、新ルールを新たに適用することで旧ルールの互換性が無くなることを指します。参加者の合意が１つに纏まれば良いです（例：2016 年香港 Bitfinex 事件）が、参加者の意見が割れた結果、旧ルール支持派と新ルール支持派が分裂することもあります。例えば、2016 年にイーサリアム派とイーサリアム・

クラッシック派に分岐したDao事件がこれです（2017年にビットコインもビットコインとビットコインキャッシュに分岐）。恣意的な取引の介入を排除するブロックチェーンの精神からは本来は行なわない処理ですが、実際には何度か起きてしまうため、仮想通貨の信頼性に疑問を呈する意見もあります。

さて、現在の銀行預金取引であれば、仮に詐欺が原因で振込が行われた場合であっても、相手方の銀行口座に入金すると支払義務が完了します。そうでないと取引が安全に行われないので、「取引保護」の観点からそうなっております。つまり、巻き戻しは行わない。それに対して、ブロックチェーンの場合は、システム的に巻戻しが困難なのに加えて、この支払義務の完了時点というのが不明確であります。すると、従来の銀行預金取引に比べると、債権債務関係が不明確になり、混乱を来し得ます。参加者が合意すると、ハードフォークを実施することがありますが、この場合には、合意できるかどうか分かりません。

例えば、香港で起きたBitfinex事件は、香港の仮想通貨運営会社が資産の4割を盗まれた際、会社が損失分を穴埋めして、何とか合意を取り付けたという事件です。Bitfinexが損失分を補填したからよかったですが、補填しなかったら、仮想通貨保有者の中で如何に損失分担を図るかを巡り、合意を取り付けられなかった可能性が高いでしょう。そうなると、仮想通貨の私法上の性格が各国ともにまだ不明確な現状にあっては、混乱は避けられません。私法上の性格については、日本にあったビットコイン取引所Mt.Gox破綻を契機に、各国の私法上の検討が進み、様々な議論がありますが、まだ明確な位置づけには至っていません。

ここで、ハードフォークがそもそもなぜ起こるのかを考えてみると、「ビッドコインって、信頼性の確保された暗号技術によって守られたシステムだったんじゃないの？」という疑問が生じます。信頼性が確保されたはずなのに、現実に幾つも事件は起きている。その理由は、システム会社、仮想通貨の取引所自体のシステムが脆弱だったわけで、暗号技術そのものは安全だと説明されています（但し、寶木先生がご報告されたように、量子コンピュータが開発されれば、現在採用されている公開鍵暗号技術では危険です）。ただ、そうは言っても使う側からすると仮想通貨システム全体でみれば、やはり危ないシステムではないかという疑問も残ります。資金決済法改正で、仮想通貨取引所にシステムの安全管理が義務付けられましたが、それで十分なのか、注視していく必要があります。

一方、今度は金融商品取引に用いる場合ですが、法律問題が絡むフロント取引ではなくて、会計帳簿等に絡むポスト取引に活用されています。さらに、証券保管振替機構においてブロックチェーン化する動きがあります。

次は、公法上の論点、つまり民対国であります。ブロックチェーンと公法との関係といっても、ブロックチェーンの現在の応用例としてはビットコインなどの仮想通貨が中心なので、仮想通貨と国家との関係に絞って話をしたいと思います。

まず、資金洗浄対策、すなわちマネロン対策です。ビットコイン利用のマネロン事件は、2013

年にアメリカで起きたシルクロード事件が有名で、今年１月には日本でも起きました。仮想通貨に限った話ではないのですが、国際組織 FATF の評価によれば、日本のマネロン対策は遅れており、国際基準（FATF 勧告）を守ってないと名指しで批判されてきました。その理由は、今年盛んに審議された例の共謀罪であります。国際組織犯罪防止条約を批准していないのが FATF による日本批判の主因であり、批准できない理由は日本が国内法で共謀罪を導入していなかったからです（本報告後に日本政府は組織犯罪処罰法改正の形で共謀罪を導入した）。

この共謀罪を巡っては確かに賛否両論あります。特に早稲田の法学部の先生にも、反対の方が大勢いらっしゃいます。他国とはやや異なる日本の法文化の特徴に、憲法上の概念である「立法事実」があります。立法に必要な事実が過去に行われていることが確認されれば、立法してもいいという考え方です。共謀罪の場合、そうした立法事実は見当たらないというのが反対論の根拠の１つです。しかし、マネロンのように将来何が起こるか分からない事態に対処する場合に、立法事実はそれほど重要でしょうか？ビットコインにより匿名で決済することが容易になり、これが闇ウェブ等で地下犯罪を横行させています。このような技術発展によって高度化する犯罪に対応すべき法律に、過去にこういうことが起こったからという事実を厳密に求め続けること自体が、もう古いのではないかと私は思います。

少し脱線しましたが、マネロン対策については、FATF 基準を遵守するためのコンプライアンスのコストがあまりかかり過ぎてしまっています。このため、ビットコインとかブロックチェーン取引を新たにやろうとする場合にも障害になりかねません。それについては、FATF の基準を読みますと、リスクベースアプローチという考えがあります。リスクが高いところにエネルギーを投入しなさいとなっております。今はビットコインよりも、不動産とか商取引を仮想したマネロンのほうが多いですので、そこをうまく説明して、切り抜けていくべきではないかと思っております。

その他、消費者に対する啓蒙政策とか、差押え、押収の技術的可能性などの問題があります。今の段階では、仮想通貨、ブロックチェーン以外の他の資産があれば、そこから実行するということも考えられますが、今後、ブロックチェーン資産以外に資産がない場合には問題が顕著になるでしょう。

他方で、制度間競争という側面もあります。日本も含めて各国がいかにブロックチェーン市場を育てるかという競争です。そのためには、国の法律がそのブロックチェーン取引を育成するためにいかに効率的かが重要となります。例えば、イギリス等に倣って、一定期間規制を緩和して新しい取引の実施を許容する「レギュレタリー・サンドボックス」というやり方もあります。なお、英米法と比べてみた場合、日本には先に指摘した「立法事実」のように、イノベーションに対して法的な対応が遅い仕組みが存在するのではという課題があります。

最後に、日本の方策についてお話しします。

まず、資金決済法の中には既に様々な仮想通貨、資金決済、電子マネー類似業務が書かれており、複雑に入り組んでいます。この結果、新しい取引を開始するに当たって、思わぬ部分で追加的な規

制コストを課される可能性があり、それが新規参入の障害となり得ることが指摘されてきました。従って、今後これを立法で整理し簡明化する必要があります。一方、立法に頼らずとも、すぐ実施できることも幾つかあります。

例えば、時間認証です。例えば、日銀がタイムスタンプを発行する対策です。ビットコインの取引が10分後にしか確定しないとしても、法律上はある時点で確定したことにする必要があります。そこで、公的機関としての信頼のある日銀が電子的に、いつ取引をしたかを認証する業務を行うことが考えられます。あるいは、シンガポールやカナダなどの中央銀行が最も開発に積極的ですが、日銀が仮想通貨（デジタル円）を発行するということも考えられます。法定通貨そのものの円が仮想通貨化してくれれば、物と金の同時決済、証券と資金の同時決済、さらには差押え、徴税、金融政策等も非常にスムーズに行われます。但し、それが過剰な国家管理に繋がるとすれば新たな問題も生じ得ます。

しかし、何といっても、国ではなく民、すなわちビジネスの発展が重要です。マロンコインでもMUFGコインでも、こういう民間の商品開発をどんどん活発に開発していって、民間がリスクを取ってブロックチェーン取引を活発化すべきと思います。例えば、Googleを見てみると、訴訟をやりながらどんどんビジネスを発展させてきた。ああいう精神を日本も見習っていくべきと思います。法律家にとっては、確率の低い事象をあれこれ細かく議論して考慮してもらえれば、自分の株が上がりますので、いろいろ言います。しかし、経営サイドに立てば、やはり法律的にグレーな部分で新規ビジネスを開拓していかなければならない面もあるので、少なくとも法律面からブロックチェーンの発展に今の段階で黒とする論理は見出せないと思います。

以上で私の報告を終わります。ご清聴ありがとうございました。

講演５

「ブロックチェーンは経済社会をどう変えるか」

早稲田大学商学学術院　教授　佐々木　宏夫

市場の役割について：

ここでは経済学者の立場で、ブロックチェーンや、さらにはこれとある程度の関係を持ちながら最近急速に発達しているIoT（Internet of Things：モノのインターネット）などが、どのようにわれわれの経済に影響をもたらすかといったことを考えてみたいと思います。

実はこういった情報テクノロジーの影響については、ビジネスや経営への影響の話はよく議論されていると思いますが、私もこの分野の勉強を始めてからつくづく思うのは、ビジネスよりもうちょっと幅の広い、経済システムや社会システムなどへの影響という議論はあまりなされてこなかったような気がします。ここでは、そのあたりへの影響やインパクトといったことについて考えてみたいと思います。特に、AIの発達なども含めた技術革新には非常に興味深い点も多々ありますので、そう言ったことについてもお話ししたいと思います。

ところが、経済学者が一番フォーカスしなければいけない対象は市場ですが、まず市場とは何か？そしてその機能や役割は何か？といったことについて整理しておきたいと思います。

さて、この世の中にはわれわれが欲しいものはたくさんありますが、それらは必ずしもわれわれの欲求を完全に充足するだけの量は存在していません。このような場合に、その財は希少だといいますが、この希少な資源をどのように人々や企業の間に分ける、つまり配分していくのかという問題を考えるときに、われわれはときに市場を使うわけです。

例えば、今日が非常に暑い日だったとして、ここにいる人たちはみんな水が欲しくてしょうがない。ここには、ペットボトルの水が１本だけある。そのときに、１本しかない水を欲しい人がたくさんいたらどうするかという問題です。配分に際して喧嘩が起きないようにするために、いろんな社会的なデバイスがあります。例えば、裁判で調停して決めるなどというやり方もあるかもしれません。しかし、こういう場合に裁判のような手間暇のかかる仕組みを使わなくてもオークションをやれば、比較的スムーズに資源配分ができるわけです。つまり、最初10円から始めて、買い手を募る。もちろん提示される価格が安いときには沢山の人が飼いたいと言って手を上げるかもしれません。しかし、だんだん値段を上げていくにつれて買いたいと希望する人の数は減っていくでしょう。そして、さらに値を上げて最後の１人になるまでやります。その値段が150円だとしたら、「それでは、150円でこの水をお渡ししましょう」という形で資源配分が決まることになります。

オークションに代表されるような市場を使って資源配分を行うメリットは、少なくとも４つあります。

第１のメリットは、人々はそのメカニズムへの参加を強制されないことです。つまり、関心のない人はオークションに加わらなければいい。ですから、参加したいと思った人が自由意志で参加できるのが市場なのです。

第２のメリットは、市場の取引は基本的に人々の自発的な意志に基づいて行われますから、その結果についての恨みとか不満が残らないことです。つまり、オークションをやって、最後に150円になって、１人だけに絞られたということは、例えば130円でだったら買ってもいいと思った人は、150円も出す気にはならないわけですから、自発的にこの水の購入をあきらめることができるわけです。

第３のメリットは、市場を利用するためのコストは比較的安いということです。実際のところ、市場を利用するためにはある程度のコストがかかります。例えば、証券市場を使えば株式の売買手数料を取られます。ですからコストはゼロではありませんが、弁護士費用だけでも巨額に上る裁判などと比べれば、市場の利用コストはタダ同然でしょう。

市場を使う第４のメリットは、市場では効率的な資源配分が達成できることです。ペットボトルの水の例でいえば、オークションでこの水を手に入れることのできる人は、それに一番有用性を見出している人です。他の人は150円の価値まではないと考えているから途中で購入を諦めたのですが、最後に残った人は一番高い価値を見いだしているからこそ高い値段でも購入しようと思ったわけです。これが効率性の意味です。つまり、市場にはそこで取引される財に最も高い価値、最も高い有用性を見いだした人がその財の持ち主になるという意味での効率性を実現させるというメリットがあるのです。

それに対して、市場以外の資源配分メカニズムでは、この４つのメリットをすべて実現させることは難しいのです。例えば、裁判所の判決で水を利用する権利を獲得させることを考えてみましょう。この場合には、まず参加が強制される可能性があります。つまり、訴えられた人は、もし裁判所に出頭しなければ自分に不利な判決が出てしまうかもしれませんから、本当は嫌でも裁判所行かなければならなりません。

また、判決が不本意なものであれば、結果に不満や恨みが残ることがあります。

それから、先ほども述べたように、弁護士費用などこの仕組みを利用する費用がとても高いです。

最後に、結果が効率的である保証がありません。裁判は、その合法性や正義といった観点で裁きますから、本当はその水にたいした価値や有用性を見出してない人であっても、その人に権利があるということになるかもしれません。

これらのことから、市場機構というのは非常に良いメカニズムだということをここで確認しておきたいと思います。

しかし、市場は常にわれわれの社会でうまく機能しているのかというと、実は「市場の失敗」と

呼ばれる幾つかの否定的な現象があって、必ずしもうまくいかない領域がたくさんあるのです。その場合には、市場を使わずに、政府が介入するなど、いろいろなやり方で問題解決を図っていくことになります。

市場の失敗の典型例としてよく挙げられるのが、このスライドに書いた四つです。その一つは、「情報の非対称性」です。これは、売り手と買い手との間で持っている情報が違う状態です。例えば、株式市場では会社の内部情報に通じている人はその会社の将来性をよく分かっていますが、会社の内情に通じていない一般の投資家は必ずしもよく分かっていない。このような情報の非対称性があると、情報を持った人と持たない人との間で不公平が生じ、結果としてその市場で成立する価格は公正なものでなくなってしまいます。このように情報の非対称性を放置すると市場はうまく機能しなくなってしまうのです。したがって、内部情報に通じているインサイダーによる株式の売買を法が禁じているのは、市場の失敗の困難を克服するという点での合理性があるのです。

これ以外にも、公害などの「外部性」があります。また、「公共財」という、いったん供給されると全ての人が同時に消費できてしまうという性質を持つ財（放送サービスなど）の場合には、お金払っても払わなくても消費することができてしまいますから、皆が他人が払ったコストにただ乗り（フリーライド）しようとする動機を持ってしまいます。そのため資源配分がうまくいかなくなるわけです。最後に、「不完全競争」が市場の失敗の典型例として挙げられます。

これらの市場の失敗の中でも、現実社会で特に深刻な問題になりがちなのは、先ほど説明した情報の非対称性です。私は昨年秋まで会計研究科長を務めておりましたが、公認会計士の監査制度がなぜ必要なのかと言うと、投資家と経営者などの企業内部の人たちの間の情報量の格差があるからです。そのような情報格差を放置しておくと株式市場の健全な発展を損なうので、公益を代表する公認会計士が一般投資家に代わって企業の内情を調べ、情報格差を解消するという意義があるわけです。

また、一般的に言って、市場の失敗のある場合には、それを解消させるために政府が市場に介入すること正当化される場合もあるということにも留意したいと思います。

ブロックチェーンと誘因問題：

以上述べた市場についての認識を前提として、ブロックチェーンやその他の情報技術の発展の影響を考えたときに生じる幾つかの論点を、５つに要約してご紹介したいと思います。

一つは、ブロックチェーン自体にまつわる問題です。ブロックチェーンは、必ずしも技術的に確立したものではないという気がしております。特に重要なことは、誘引問題、つまり人々が嘘をつかずに正直にシステムに参加するかという問題です。

例えばビットコインで考えますと、分散的にデータを保持している人がたくさんいて、マイニングを行う企業が非常にたくさんいるということがシステムがうまく機能するための前提条件です。

完全競争市場では、非常にたくさんのプレーヤー（企業や消費者）がいることが重要ですが、ビットコインのアイデアというのも競争市場のアイデアと非常に似ておりまして、たくさんの人の目があるのでなかなかズルができないし、各個人の全体に占める割合は非常に小さいので、ズルができたとしてもそこから得られる利益は非常に小さいので、いずれにせよズルはほとんどできないということになるわけです。

ところが、ビットコインに関しては、まず採掘が曲者であります。確かに初期には沢山の人が採掘に参加していたようなのですが、競争の進展に伴って採掘するためのコストがどんどんかかるようになってきています。最近では体育館のような巨大な施設に何万台ものコンピュータを置いて計算するような採掘会社もあるようでして、コストをかけないと実は採掘競争に勝てなくなっております。その結果、採掘する人（会社）が非常に限られてきており、寡占化が起きております。

また、先ほどパブリック型か非パブリック型かという話がありましたが、特にパブリック型の場合には、各コンピュータを保有するプレーヤーが、お互いにデータを分散所有するインセンティブや動機がどこにあるのかという疑問があります。

どういうことかといいますと、ブロックチェーンに書いてある膨大な情報のほとんどは自分と関係ない情報です。それをみんなが自分のコンピュータに保管していくことで初めて正しい情報の保全が確保されるわけです。経済学的にいえば、そこで保全されるデータセットは公共財の側面を持っております。そうすると、先ほど申し上げたように公共財はフリーライダー問題を引き起こし、市場の失敗の原因となります。すなわち、莫大な情報を各人のコンピュータに入れて監視するためには、それなりにコストがかかります。メモリの容量もたくさん食います。電気代も食うかもしません。そうすると、多くの人々は、皆が情報を保全することは大事だということは分かっていても、自分がわざわざコストを払ってまでして情報を自分のコンピュータに置かなくてもいいということになります。結局、皆がそう思ったらどうなるのかというと、場合によっては誰も自分のコンピュータにブロックチェーンのデータを保管しようとしなくなるか、あるいは保管する人が出たとしても、コストをかけてわざわざそういう事をする人は下心のある人ばかりになってしまうのではないかというような問題もあります。

こういったブロックチェーンにまつわるフリーライダー問題についてはほとんど議論されてこなかったような気がします。ですから、特にパブリック型の場合には、本当にうまく機能するのかという疑問が生じてきます。そうすると、むしろある程度閉鎖的なシステムにして、比較的情報をみんなで共有して保有することに意味があるような仕組み、つまり、非常に限定的なブロックチェーンを利用した方がいいのかもしれないという感じもします。

経済学視点と工学的視点：

さて、第２の論点に話を進める前に、ブロックチェーンなどの勉強を通じて経済学者として感じ

たことを一つお話ししたいと思います。

私は経済学の中でも特にメカニズムデザインの研究をしていますが、そこでは人々がうそをつけない資源配分の仕組みを作ることが重要なテーマの一つになっています。このような絶対に嘘をつけない資源配分メカニズムは「耐戦略的」であると言われています。ところがこの「絶対にウソがつけない」という条件は厳しすぎて、そういうメカニズムは作れないという結論になってしまう（不可能性定理が成立）ことが多いのです。

ところが、興味深いことに、工学の研究者（そしてコンピュータ技術開発の実務家）は、人がウソをつくのは仕方がないことだと割り切った上で、「あまり実害のないウソ」、すなわちウソをつける可能性が低いシステムを作ろうとするわけです。このように条件を緩めると、絶対に嘘をつかせないという厳しい条件の下で不可能性定理が成立してしまったケースでも、ある程度嘘がつけないメカニズムを作ることができるわけです。

先ほどの宝木さんからお話のあったゼロ知識証明にしても、情報を持っているが、その情報の中身は開示しないまま、「この人は本当に情報を持っているようだ」という確信を第三者に確信させることのできる素晴らしい技術です。ただし、厳密にいうと、これは数学的・論理的な「証明」ではありません。つまり、「絶対に情報を持っている」ということを証明するのではなくて、「情報を持っている蓋然性が非常に高いですよ」という証明だと思います。

この点については、工学系の人たちの考え方は素晴らしいなと思っています。実務上、実用上は蓋然性の高さを示せば十分なことが多いからです。

もっとも、個人的な感想としては、ブロックチェーンの研究・開発は、先ほど述べたような誘引構造の解析などが体系的に行われておらず、経験則でやっている部分が多いとは思います。例えば、ビットコインで言えば、今までにあまりおかしなシステムの誤動作や不正などがなかったから、たぶん平気だろうと考えている気配を感じます。

例えば、ビットコインにおけるプルーフ・オブ・ワークが、ビットコインを発行するための労力の代償として機能するのはよく分かりますが、それによって本当にうそがつかれないことが証明されているかどうかとなると、我々ゲーム理論家の目から見るとちょっと怪しいところはたくさんあります。このあたりに、われわれの経済学者やゲーム理論家が研究するための課題は、たくさんあるなという気がしております。

市場の失敗の克服：

さて、話を経済学的な論点に戻しまして、二つ目の論点についてお話ししたいと思います。それは、最近の情報テクノロジーの進歩、すなわちブロックチェーンをはじめとしてIoTやAIの発展によって、市場の失敗の中でも特に情報の非対称性がかなり克服されてしまうかもしれないという論点です。

例えば、保険サービスの中にはブロックチェーンが使える面白い領域がいくつかあるという話題があります。

実は保険におけるリスクには二種類があります。一つは被保険者自身が直面している元来のリスクです。ひょっとしたら自動車事故に遭うかもしれない、死ぬかもしれないといった類のリスクです。このような元来のリスクに加えて、保険市場には深刻な情報の非対称性がもたらすリスクがあります。保険加入者がどれぐらいリスキーな人かということを、保険会社はちゃんと把握できません。しかし、その一方で保険加入者は自分のことなので、自分がどの程度のリスクに直面しているかをある程度正確に把握しています。このような情報の非対称性に起因する問題です。

こういう情報の非対称性があると、「逆選択」や「モラルハザード」といった困った問題が引き起こされることはよく知られていますが、保険会社はこういう問題に対処するために苦労しています。例えば、保険加入者のリスクの程度と一定の関係のある指標を「シグナル」と言います。自動車保険で年齢別に保険料を変えていますが、この場合の年齢はシグナルの１つです。保険会社は、いろいろと考えて、妥当なシグナルを見つけようとしています。それでも、それを見れば加入者のリスクの程度が完璧に分かってしまうようなシグナルを見つけることは不可能です。

しかし、IoT やブロックチェーンなどの技術が発展してきますと、実はこの種の情報の非対称性はかなり克服されてしまう可能性があります。例えば、車の運転をしていて急ブレーキを踏む回数がすごく多い人がいたとしたら、その人が事故を起こす可能性は高いと思うのは自然でしょう。つまり、急ブレーキを頻繁に踏む運転者はリスクの高いドライバーである可能性が高いのです。このような場合に、急ブレーキを踏むたびにその記録が無線を介してブロックチェーンなどを活用したデータベースに情報として蓄積される、と言うようなことが可能になれば、その情報を利用することで保険会社は加入者のリスクの程度をかなり正確に把握できるようになるかも知れません。

こういう情報が蓄積されていけば、各個人が直面しているリスクの程度がある程度正確に識別できるようになる可能性があります。このようにして保険市場における売り手と買い手の間の情報の非対称性は徐々に解消されていき、保険会社は保険固有のリスクだけにフォーカスして料率（価格）設定をすれば良いと言う事態になって行くかもしれません。

もっとも自動車へのこういう技術の実装が進んでいくと、個人の運転に関するリスク情報を一番たくさん持っているのは自動車会社だということにもなりかねません。そうなると、保険会社でなくて自動車会社が保険をやるというような時代が到来する可能性もゼロではないでしょう。つまり情報テクノロジーの発展によって情報の非対象性がかなり解消される代わりに、違った問題が起きてくるということなどもあるかもしれません。

次に、情報の非対称性の解消のもう一つの例として、シェアリングエコノミーを取り上げたいと思います。つまり、昨今の情報技術の非常に優れた応用例の一つとして、例えば Uber というカーシェアリングの仕組みがあります。

実はこれに類したお互いに何かを融通するという仕組みは、昔からありました。例えば、田舎町

でおばあちゃんが病院に行くのに困っていたら、隣の息子が「おばあちゃん、これから病院の近くまで行く用事があるから乗せてってやるよ」といって車に乗せてやるというようなことは昔からよくあったわけです。そして、おばあちゃんはその場でお礼をしなくても、自分の畑でスイカが採れたらお礼を兼ねてそのスイカを隣の息子にお裾分けしたりするわけです。

ただ、こういうことがスムーズに出来るのは、お互いの顔が見える小さな田舎町ならではのことだとも言えるかも知れません。互いの顔が見えない、つまり匿名性が支配している大都会でそれをスムーズに行うのは結構難しいでしょう。都会でおばあちゃんが病院に行こうとして車に乗っている若い男が「乗りませんか」と声をかけてくれたとしても、おいそれに乗るわけにはいかないでしょう。車に乗ったとたんに法外な料金を支払えと迫られるおそれがないとはいえません。また、逆に車を運転している人も、見ず知らずの人が大きな荷物を抱えてヨタヨタとあるいていても、なかなか声をかけづらいでしょう。乗ったとたんに強盗に豹変する人だっていないとは限りません。このように考えると、匿名性が支配している都会では、なかなか助け合い仕組みのようなものをうまく作れないわけです。

このように都会で助け合いが難しくなる理由も、情報の非対称性にあるわけです。車に乗ろうとする人が本当に善良な人であるのかどうかがわからないし、車に乗る方にとっても運転者がどんな人かがわからない。このような情報の非対称性があるので、タクシーの免許制にはそれなりに合理的な理由があるわけです。つまり、免許制の下では、国家が一律にタクシー営業を禁止した上で、特定の審査に受かった人をだけに免許を与えて運転を許すわけです。こうすることで、少なくとも車に乗る側は余計な心配をしなくてすむことになります。

これに対して、Uber の仕組みの元では、乗客はある車に乗った後に５段階での評価を求められます。このような評価情報が蓄積していくことで、問題の多い運転手は駆逐されてしまいますし、運転手自身良い評価を得ることのメリットを自覚しますから、おかしな行動に走る動機が削がれてしまいます。客の側も車の中でおかしなことをすれば、それが報告されて今後 Uber を使えなくなってしまうかもしれませんから、やはりおかしなことはできなくなる。つまり、このようなシステム上の評価システムを通じて情報の非対称性はほとんどなくなりますから、そうなるとそもそもタクシー営業を免許制の下で規制する必要性はあるのか、という疑問が出てくるわけです。

このように考えると、情報の非対称性絡みの市場の失敗は、情報テクノロジーの発展によってかなり解消されるのではないかという気がしています。

社会における対立の激化：

３つ目の論点として考える必要があるのは、社会的に様々な対立がこれから生まれてくる可能性があるという点です。官民の対立もあれば、民民の対立もあり得ます。さらには、富める者と貧しい者の対立、あるいは情報技術にアクセスできるものとアクセスできないものの対立など、さまざ

まな対立が生まれる可能性があると思います。もっとも、現在は急速に新技術が導入された過渡期ですので、ひょっとしたら今述べたような対立も過渡的な現象で、いずれは安定的になるかもしれませんが、過渡的か否かはともかくとして、対立に起因するさまざまな社会的なコンフリクトが起きる可能性があると思います。

官と民の対立の問題でいえば、民間はいともたやすく国境を越えてしまうことができますが、国家は国境に束縛されています。この矛盾がだんだん顕在化し、激化していく可能性があります。例えば、国境をたやすく超えるということでは、先ほどのSAPさんのアリバです。あれは、ある種の世界的なレベルでの物々交換の仕組みと解することができます。昔からわれわれ経済学者は、広範な領域での物々交換というのは「欲望の二重の一致」ができないから無理だと言ってきたのですけど、今のネットワーク技術を使うと、世界規模での物々交換も十分射程内に入ってきます。そうなると、例えばお金の介在無しに物々交換されてしまったときに、どうやって課税するのか？とか、そもそもそこでどのような所得が発生したといえるのか？、あるいは日本の会社とアメリカの会社が直接に物々交換したときにどこが課税当局になるのか？など、実はいろいろな問題が出てくるような気がします。

それから、官と民という点ではやはり仮想通貨が一つのネックになる可能性があります。先ほど宝木さんから、ビットコインは世界で１兆円ぐらいの規模だから大目に見てもらっているとおっしゃいましたが、まさにそのとおりだと思います。仮想通貨が例えば国家の通貨を凌ぐような存在になってきたときには、基軸通貨国のアメリカは徹底的につぶしにかかるだろうと思います。アメリカは基軸通貨国であるということによって国際社会で大きな「力」を獲得しています。つまり、基軸通貨国であるメリットは非常に大きいですから、仮想通貨によって基軸通貨国の立場が脅かされるのならば、当然にそれをつぶしにかかるだろうと思います。アメリカ以外の国にしても、例えば日本でも、日本で日本銀行券よりも仮想通貨の方が信用され、流通するような自体になることを政府も日銀も決して歓迎しないでしょう。したがって、そこでも徹底的につぶしにかかるかもしれません。

それから、国によってはむしろ積極的に仮想通貨を歓迎してドル中心の経済に反旗を翻すところも出現するかも知れません。そうなると、今度は国と国との通貨競争が起きる可能性だってあるわけであります。

先ほど、日銀が仮想通貨を発行するという話がどなたかからありましたが、将来的なシナリオとしては、私はアメリカが仮想通貨を発行する可能性もあると思います。つまり、米ドルが仮想通貨化するわけです。もしそういうことになると、国境を超えた通貨が生まれてくるわけですから、日本国内でも別に日本円で決済しなければならない理由はなくなってきます。むしろこれだけ経済がグローバル化していくと、海外のサービスや物品を国内で容易に利用できる環境はどんどん整備されていきますから、消費者や企業にとっても為替のリスクの心配がないドル決済が好まれるようになるかもしれません。そうなると、日銀と米国連邦準備制度との間の戦いが起きる可能性がありま

す。それから、もしドルが仮想通貨化すると、仮想通貨の特性としてほぼ無コストで送金ができてしまいますから、そういう点では民間の銀行にとっては大きな脅威だろうと思います。つまり、そうなると仮想通貨でドルを供給する連邦準備銀行（あるいは、アメリカ政府）と民間銀行との戦いも生じるかもしれません。

それから、民と民の対立ですが、これはもういろいろあると思います。例えば、先ほどお話したUberを見ればわかるように、タクシードライバーとタクシー業者との対立、消費者とタクシー業者の対立等が生じるでしょう。あるいは、損保会社と自動車会社の対立、あるいは民間銀行と民間が発行する仮想通貨の対立なども生じるかも知れません。実は、大学も無縁ではありません。アメリカの一流大学は、ネット授業ななどを使いながら世界中から優秀な学生を、いわば「一本釣り」でリクルートしています。そういう中で、それでは私どもの大学は、どうやって優秀な学生を確保していったらいいのか、という問題なども出てきています。

効率と公平の問題：

第4の論点は効率性や公平性に関することです。これはある意味経済学の伝統的な論点でありますけれども、「効率と公平のトレードオフ（対立）」という問題があります。先ほど申し上げたように、市場は効率的な資源配分を担保するシステムです。ところが、効率性と公平性が両立しないという問題が「効率と公平のトレードオフ」ですが、市場はたしかに効率的な生産を実現させるのですが、そこで得られた資源配分が公平なものである保証はないのです。

公平性には二つの観点があります。一つは、その結果の公平（平等）です。要するに金持ちと貧乏人の差をできるだけ小さくしましょうということです。もう一つは、機会の公平（均等）です。要するに、全ての人々が同じ条件で競争できるようにしましょうということです。

今のテクノロジーの発展は、この両方の観点から見た公平性に対して深刻な問題を惹起する可能性があります。

第一に、結果の公平ということについてです。

先ほども述べたように、情報テクノロジーの発展に伴って市場の失敗はどんどん減ってきております。そうなると政府の役割もだいぶ変わってこざるを得ないことになります。これまでは、市場に関して政府の重要な役割の一つは、市場の失敗の是正という点にありました。そのために、例えば公認会計士の法定監査の制度を作るとか、あるいはタクシーの免許制度のように様々な形で市場に介入することが必要だったわけです。そのあたりの必要性が薄れてくると、後で夜警国家という話もいたしますが、非常に極端なケースだと、ピュアな資本主義経済に近いものが生まれてきてしまう可能性があります。しかし、市場は不公平を是正する力を持ちませんから、社会に豊かな人と貧しい人の差は依然として残ることになります。そうなると、累進課税制度のようなもので所得の再分配を積極的に行って、結果の不平等を是正する政策の重要性はそういう時代になっても必要な

わけです。つまり、政府の仕事の中で、所得再分配の重要性が増してくる可能性が高いのです。

今までも、基本的に累進課税制度はそういうものですが、ただ政府が市場の失敗の是正のためにさまざまな仕事をしているときには、税はそういう多様な目的のために徴収されているわけですから、高額な税金を支払う人の不満はそう大きくなかったかもしれません。しかし、所得再分配が政府のより重要な機能になるに連れて、税を負担する人の意識の中には再分配がクローズアップされることになります。そうなると富裕層はなかなか納得しなくなるかもしれません。その結果、富裕層は海外に脱出するなど、いろいろな問題が出てくる可能性があります。つまり、政府がそういう点により力点を置くようになってくるにつれて、そこから納税者の反発や豊かな層と貧しい層の対立の深刻化などが生じるようになる可能性もあります。

次に、機会の公平に関わる点です。Uber が最近アメリカで非難を受けているという記事をある雑誌で読みました。なぜかというと、各消費者に対して個別に価格設定をしているようだということでした。そこで一つ出ていた例は、携帯電話のバッテリーの残量がゼロに近くなっている人は、高い値段をオファーしてもアクセプトする可能性が高いので、そういう人には高い価格をオファーするのだそうです。その他、消費者一人一人の状況を見ながら価格付けをしてくというようなことをやっているようだ、ということでした。

経済学で言いますと、これは完全な価格差別ということにあたります。

価格差別というと、普通思い浮かべるのは鉄道の学割やシニア割引のようなものです。これは、たとえば学生と社会人とでは価格の需要弾力性に違いがあるので、その差に着目しながら価格付けをしていこうというやり方です。学割などは、消費者をせいぜい２つのタイプに分けて差別価格を適用するという程度のものですから、それほど弊害はないのですが、これを消費者ごとに細かく需要構造の違いを把握して、個別に価格設定するというのが完全な価格差別です。差別価格の中でも個別にやるっていうのは確かに理論的には今までありました。

完全な価格差別は経済学の教科書に必ず載っている独占力の行使の形態ですが、実際問題として個人ごとの需要構造の違いを把握するなどと言うことは至難の業ですから、教科書には書いてあっても実際にはやれるはずのないものと考えられてきました。

しかし、確かに情報技術とネットワークをうまく使うと、Uber がやったように、個別消費者の需要の構造をかなり細かく把握できるようになります。そうなると、完全な価格差別もしくはそれに近い価格付けが可能になってくるのです。

実は、これも経済学の教科書に書いてあることですが、完全な差別価格をすると消費者の利益（これを消費者余剰と言います）はすべて Uber に取られてしまいますが、今までの消費者の利益プラス企業の利益（これを生産者余剰と言います）を合わせたものが Uber の利益になりますから、実は Uber にとっては、「消費者余剰＋生産者余剰」を最大化することが利益になります。つまり、この場合でも効率的な資源配分が達成されるのです。

ここで問題になってくるのは、効率性は担保されるが、公平性が担保されなくなってしまうとい

うことなのです。つまり消費者が全ての消費者余剰を取られてしまうという意味で、消費者が制度上極端な不利益を得るという不公平が出てきてしまうのです。

そうなると次の疑問が出てきます。つまり、競争維持政策の意義、すなわち独占禁止法がいったい何のためにあるのかという疑問です。

この場合に重要なのは、消費者保護の論点を整理する必要があるだけでなく、プライバシー保護というものについても考える必要が出てきます。つまり、Uberのような事例を見ると、プライバシー保護は必ずしも倫理的な観点から必要とされるだけでなく、他人のプライバシーを利用して企業が金を稼いでいいのかという問題となるわけです。

つまり、携帯電話の電池残量をのぞき見するというようなプライバシーの侵害によって、消費者の利益が損なわれてしまうという経済問題が発生する可能性があるのです。先ほどの宝木先生のご発表を僕なりに理解すれば、プライバシー保護と公正さを担保するための監査機能のバランスをどこで取るのかということです。そのためのテクノロジーを開発しておられるというふうに理解しましたが、まさにプライバシー保護というのは、これから重要な問題になってくる可能性がという気がしております。

マクロ経済学の黄昏：

第５の論点です。これについてはあえてマクロ経済学者に対して挑発的な言い方をしまして、「マクロ経済学の黄昏」という題にしましたが、マクロ経済学はこの急激な技術進歩の中で大きく変わらざるを得なくなってくるという気がしております。

アダム・スミスの『国富論』という200年前の有名な本がありますが、その冒頭に「ピン工場の例」があります。虫ピンのようなピンを作る工場があって、ある人は鋳型を造ることに専念する、ある人はできたピンを磨くことに専念する、ある人は鉄を溶かすことに専念するという完全な分業をしている。分業をしている結果、１日に何千本もピンが作れるけれど、それを１人がやっていたら絶対に作れないという話です。つまり、分業がいかに生産性を上げるのかということをスミスは言っているわけです。

ところがアダム・スミスの本を読んでいると非常に面白いのは、ひたすら供給サイドの話が続くのです。つまり、いかにして生産を効率的に組織して、いかにコストを下げるかということです。そして、市場での安価な取引や効率的な生産を阻害するような政府の規制を批判することに彼は終始しております。こういう風に理解するとアダム･スミスの経済学はサプライサイドの経済学です。

なぜ彼がそういう主張をするのかと言えば、当時のイギリスは、世界中に植民地を持っていて、市場がどんどん広がっていくという環境にありました。だから需要は腐るほどあったのです。ところが供給がそれに追い付かなかった。だから効率的な供給体制を作ること、そのために不毛な規制は排除することこそが、豊かさのための条件だったのです。

ところが、マクロ経済学の歴史を見ると、このサプライサイドの考え方とディマンドサイドの考え方が交互にやって来ます。つまり、生産をどんどん効率化していくと、今度は供給過剰になってくる。そうすると今度は需要が不足してくるわけです。需要が不足してくると、どうやって需要をつくり出すかという問題が出てきます。その典型がケインズ経済学です。このように、サプライサイドに力点を置くときとディマンドサイドに力点を置くときが行ったり来たりしているのが、経済学の歴史とも言えます。

ひるがえって、それでは今の日本の状況はどちらなのか？という話になりますと、基本的には需要不足の時代ではないかと思っています。つまり、もうここ 20 年、30 年にわたってさまざまな経済政策を導入しても景気がよくならないのは、基本的には需要が足りないからだと思います。それでは、需要不足ならばケインズ経済学の処方箋でいいのかということになりますと、実はそう簡単ではないわけです。

なぜかというと、ケインズ経済学が教えてくれる方策は、基本的には財政政策と金融政策で需要を喚起するということです。ところが､財政政策はもう国債がこれだけたくさん発行されていたら、これ以上の大形の財政出動は困難です。ですから､財政政策に頼るわけには生きません。それでは、金融政策ですかという話になると、金融政策は副次的な政策です。直接需要にインパクトを与えるものではない。実際に量的緩和だとかゼロ金利だとか、さらにはマイナス金利だとか、いろいろなことをやっても、うまくいっていないわけです。そうなると、今までの伝統的なマクロ政策というのは、実はほとんど実効性を失ってきているように思えます。

そこでいったいどうしたらいいのかというと、新しい市場を発見・発掘する以外にすべはないだろうと思います。比喩的な言い方をすれば、私は新しい大航海時代が始まったのではないかと思っております。つまり、大航海時代には、地理上の発見が行われて、当時の西欧諸国は世界中に新しい市場を見つけ出したわけです。その結果、時代的なずれは多少ありますが、アダム・スミスは需要のことを気にせずにサプライサイドエコノミクスを主張できたのです。

先ほども述べましたように、一方において需要が不足している現代において、財政政策も金融政策も使えないのならば、かつての大航海時代と同様に新たな市場を発見しなければならないと思います。

それでは発見する市場はどこにあるのかといえば、それは今まで規制の輪の中でがんじがらめに縛られていたところ､すなわち市場がなかったところに市場を作ることしかないわけです。例えば、Uber にも問題があることは確かですが、その一方で Uber がタクシー規制に風穴を開けて新しい市場を作り出したことは否定できません。あるいは、アップルは iPhone や iPad によって、アプリケーションのみならず、音楽や映画、書籍などの新しい需要を掘り起こしたのです。このように今の経済をよくするためには、無用な規制を出来るだけ廃して新しい市場を掘り起こさなきゃいけないのではないかという気がします。

もう１つマクロ経済学にとってむしろ大きな問題は、マクロ経済学で考えてきた貨幣の概念がど

うも危なくなってきているような気がしています。今までは、現金プラス銀行預金が貨幣ですよ、ということを言っていたわけですけれども、仮想通貨が現実化してくると、複数の貨幣が自然に流通しているような状況が出現する可能性が高いわけです。そういう状況下で、そもそもマネーサプライコントロールなんて、本当にできているんでしょうか？という問題があるわけです。

そういう点で言うと、もうマクロの貨幣概念をそろそろ再検討しなければいけない。さらに言えば、その延長として見ると、今までの中央銀行中心の管理通貨制というのが是か非かというあたりも、真面目に考えなきゃいけない時期に来ているのではないかという気がしています。

おわりに：

最後にまとめでございますけれども、実は経済の問題と言いながら、これからは国家とは何か？ということへの真正面の問いかけが必要になってくるのではないかという気がしています。

昔、資本主義経済の勃興機にラサールの夜警国家論というのがあって、資本主義経済が進化すると、ほとんどのものは市場で解決するようになるから、国は夜警、つまり治安維持と国防に徹すればいいという話があったわけです。ラサールは社会主義者ですから、むしろそういう方向に進む世の中を批判したわけでありますけれども、今、どんどん市場の失敗が解消されていくと、実は夜警国家に近いようなものがだんだん現実味を帯びてきている可能性はあるわけです。

そうなると、市場というものの機能や意義をもう一度考え直す必要がります。先ほどから何度も繰り返しますように、市場は効率性を担保するけれども、公平性は担保しないという問題があります。公平性を実現させるためには、市場以外の力に頼らなければいけない。そういう意味では、国家の役割というのがこれまでと違った点で重要になってくる可能性がありますということであります。

以上、私の話はこれで終わらせていただきます。どうもありがとうございました。

第三部：
パネルディスカッション

「ブロックチェーンの可能性と限界」

司会	早稲田大学商学学術院　教授	佐々木　宏夫
パネリスト	三井住友銀行 IT イノベーション推進部	竹田　達哉
	産業技術総合研究所　情報技術研究部門	宝木　和夫
	早稲田大学法務研究科　教授	久保田　隆
	SAP ジャパン　シニアディレクター	前園　曙宏

司会：

それでは、第３部パネルディスカッションに移ります。進行は、佐々木宏夫教授が務めます。佐々木先生、よろしくお願い申し上げます。

佐々木：

どうもありがとうございます。今日は私を含めると５人の報告者が発表をいたしました。それに基づいて少し議論をして深めていきたいと思います。できるだけ深い話ができれば面白いなと思っております。最初のお願いとして、発言される方には１回のご発言は３分以内ぐらいに終えていただけたらと思います。

さて、このパネルディスカッションのテーマとしては、「ブロックチェーンの可能性と限界」ということにさせていただきました。今日の発表を聞いていただいてもお分かりになると思いますが、おそらくここにいる皆さん全員がほぼ共通に認識しているのは、ブロックチェーンは非常に可能性の高いテクノロジーであるということです。ですから、世の中を変えるような潜在力を持っている可能性があるわけです。ただその一方で、マスコミなどで騒がれているような、万能のテクノロジー、あるいはゴールドラッシュをもたらすような素晴らしいテクノロジーなのかというと、そこはそうでないとも断言ないけども、まだよく見えないというのが現状だと思います。そういう点で、ここではあまり夢みたいな話ではなくて、むしろ限界の部分も含めて議論していけたら嬉しいと思っております。

ところで、実は今回は少し新しい試みがございます。クイズ番組みたいなやり方で進行していきたいと考えております。私の方であらかじめ三つの質問を用意いたしました。その答えをお手元の iPad の画面に書いていただいて、それを基にして議論をする形でやっていきたいと思います。その３つの質問の前に、少しウオーミングアップという形で、各報告者の方に今日の感想といいますか、あるいは他の方の発表に対してのコメントでも結構ですので、何か一言ずつお話しいただけたらと思います。まず久保田さんのからお願いいたします。

久保田：

法学の久保田でございます。

私は、どのご報告も非常に参考にさせていただいたのですが、最後の佐々木先生のご報告の資料の８ページ目と 14 ページ目について、法的にも大変関心を抱いたので若干コメントしたいと思います。

まず、８ページ目の工学的思考と経済学的思考です。工学的思考は確率論っぽい考え方（例えば、ファイナリティについて〇％ファイナリティという捉え方）なのに対し、経済学的思考は完全を求める考え方（例：倒産確率ゼロがファイナリティありという捉え方）だという点です。実は、法学的な思考は経済学以上に完全な世界（例:倒産確率ゼロであっても倒産法上の遡及効は及び得るが、法律上のファイナリティは遡及効も及び得ない状態を指す）を想定していて、法学からみると経済学は良い意味で少し緩い捉え方という印象を、日本銀行でエコノミストをしていた時代に感じておりましたので、経済学でも同様の問題意識がある点で非常に興味深かったです。どちらも確率論が大事だという主張は私も同じであります。

それで 14 ページのほうですが、米ドルの仮想通貨化、これは非常に面白いなと思いました。というのは、ここにも書いてありますように、米ドルが基軸通貨であることが米国の国際的なパワーの重要な源泉になっているからです。法的に言いますと、例えば、三菱銀行がイランと米ドルで取引します。アメリカはこの取引に何にも関わっていませんが、アメリカ法を域外適用してきます。すなわち、米ドルを使っているということで、コルレス関係を通じて、ニューヨークの口座を電子的に１回だけ通過します。そこで、粗っぽく言えば「電子的に一回アメリカを通過したから、アメリカ法を適用します」と言って高額な罰金や重い規制をかけてくる。米ドルは国際基軸通貨であるため、米ドル以外で取引することは難しいため、こうした事態が当たり前のように起きています。2012 年に三菱銀行はニューヨーク州裁判所から対イラン取引口座の凍結命令を受けた（その後、連邦裁判所が凍結命令を取消したため、事なきを得た）ほか、2012 年の HSPC 事件は 1560 億円、2014 年の BNP パリバ事件は 9000 億円もの大変高額な罰金を米国当局に支払わされました。

では、こうした米国の積極的な域外適用にどう対抗するか？米ドルの覇権構造を崩す代替手段はないか？ビットコインはその１つの有力な対抗手段になり得ます。ビットコインは電気代が安く、海外送金が規制されている中国で盛んですが、中国には明らかに米国への対峙パワーとしての自覚があります。すると、ビットコインや類似の仮想通貨の取引が拡大すると、電気代の安い、それこそプルーフ・オブ・ワークに主に参加してる中国あたりが国際通貨覇権を握る可能性があり、今後ますます見逃せないなと思いました。以上です。

佐々木：

ありがとうございます。それでは宝木さんはいかがでしょうか。

宝木：

簡単に、皆さん、それぞれちょっと感想を述べたいと思いますが、佐々木先生の話の石貨のご紹介ですね。以前、この事前打ち合わせで初めて聞いて大変感銘を受けたわけですけれども、石に思いを込めるということ、これは一種の信仰というか日本だと言霊、いわゆるそういうものに対する石ですね。これに行動を縛る、思いを縛るという動きですけども、暗号だとやっぱり同じようなものがありまして、大英博物館に置いてあるヒエログリフというロゼッタストーンに書いてある暗号ですね、これが資料に残っている最古の暗号ですが、これも、目的は神に捧げる言葉でした。

そういうことで人の思いというのが、いろいろ人の交流につながる、人の動きを縛る、そういうところの原始的な感覚というのが他にもあったということで、大変面白く思いますし、暗号という面が、特にこういう取引とかに使う場合も、そういう面が本質的にあるのかなと、あらためて感じた次第です。

それから、三井住友さんのお話で、実際レガシーの金融でまだまだ検討が足らないと。特に、いろいろ使った場合に、規約上というか法律上、まだまだ未解決があるということですので、こんなにまだまだなのかなとあらためて感じて、情報技術的に何かサポートをするようなことがあれば、ぜひお手伝いさせていただきたいと思いました。

その他のSAPの方は、非常にいろんなトライをしているなという感じで、動きが速いですね。さすがに外資系といいますか、あまり他の、わが国のベンダーとかサービス提供業者もうっかりしておられないなというふうに感じております。

その他いろいろいただきましたが、私としては、こういう社会を論じる場で情報技術を話させていただいて大変光栄に存じますとともに、ある意味、社会に対する責務というのをあらためて感じた次第でございます。以上です。

佐々木：

ありがとうございます。

少しコメントさせていただきますと、実は貨幣というのは歴史的にみると、宗教起源を持っていることが多いのです。日本で、例えば、不換紙幣の最初というのは伊勢神宮に関係して発行された山田羽書（はがき）というものです。どうしてもそういった呪術的な力がないと信用が確保できないのかもしれません。

それでは、次に前園さん、お願いいたします。

前園：

SAPジャパンの前園です。

本日、このような場で話させていただいてありがとうございます。感想ですけども、やはり貨幣のお話は最初にしていただいて非常に良かっと思いまします。いわゆる経済の中で価値を重んじる・

重んじない。本当にそれって価値があるのかというベースの話だったと思います。

私の実体験で一つ言えるのが、父が数年前に亡くなりましたが、その亡くなる直前に握り締めていた銀貨がありました。その銀貨のことを後で調べてみると偽物だったのですけども、当時、戦後に偽銀貨が出回っている時代がりました。それはただ父は死ぬまで本物だと思って逝ったわけですけども、要はそのときの人たちはそれは本物だと思って家宝のように持っていた。それを、今の時代で考た時には、本当に法的にそのお金が偽モノなのか本モノなのかっていうことを紐解くときの一つの要素技術としてブロックチェーンは使える可能性がある、そのような証明を過去からずっとトラッキングして改ざんができない仕組みとして実装できるし、テクノロジー的に見ると正しく使えば社会の中で証明をしてくれる仕組みが作れるものと思っています。

そういった意味で、今後の社会というのは、たぶん間違いなくデジタル化が進みますし、色々なモノがトラックされるのと。逆にそれをどういうふうにデジタルから好きな時に切り離すのか、そして繋ぐのかということなども含めブロックチェーン適用度合いも複雑化してくる中で、ここにいる我々は様々なことにチャレンジしないといけないのかなということで、今日はこういったディスカッションの場に参加させていただけることをありがたく思います。

佐々木：

ありがとうございます。それでは、最後に竹田さんにお願いいたします。

竹田：

三井住友、竹田です。

私は、仕事上いろんな要素技術、ブロックチェーンも IoT も AI も使って、金融で新しいイノベーションを生み出すということを仕事にしてますが、特にブロックチェーンの分野というのは、まだまだご説明したように技術的にも法的にも未成熟なところありますので、アカデミックな皆さんとコラボするところが大きいですし、有効なんだろうなというふうに思っています。

三井住友銀行としては、技術的な観点、あと法的な観点から、国立情報学研究所と一緒に共同研究をしていたり、アカデミックな方々のご意見も取り入れながら、ブロックチェーンを研究しているところでございます。技術的、法的論点に加えて、個人的にはおそらく、次、経営学のほうにもブロックチェーンというのがどう使われるのかというようなことが考え始められるのではないかと思います。特に、プラットフォーム理論の中でブロックチェーンをどう位置付けるかということが、そのうち研究する人も出てくるのではないかなと思っているのですけども、そういった中で早稲田のビジネススクールさんのシラバスを見ますと、「ブロックチェーンにおけるビジネス変革」という授業があるということで、さすがだなと思っているのですけども、実はスポンサーは三井住友銀行だというのがオチでございます。以上でございます。

佐々木：

ありがとうございます。それでは、最初の質問をさせていただきます。

【質問１】：ブロックチェーンで何が最も変わると思いますか？

ブロックチェーンでいったい何が一番変わると思いますか？　あるいは何が最も影響を受けると思いますか？という、ちょっと漠然とした質問かもしれませんが、皆さんがそれぞれに受け止めてくださったことを、書いてくださるとありがたいです。

先ほどのご講演では、竹田さんは改ざんできないことがとても大事だとおっしゃっておられましたし、前園さんはトレーサビリティということを非常に強調しておられたと思います。

それでは、まず竹田さんから。この「透明性が変わる」というのは、どういうことかを教えていただけませんか。

竹田：

はい。今ご指摘ありましたように、やっぱりブロックチェーンの特徴としては改ざんできないとか消せないということが一つ、大きな特徴かなと思っていまして、そのブロックチェーンを使うことで、個人や法人の行動ですとか取引が変わってくる可能性があるのではないかなと思っています。やはりブロックチェーンが使われるようになって透明性が増すということで、個人においては世の中のインセンティブの制度ですとか、そういったものが新たに設計し直されるということが起こってくるでしょうし、そのインセンティブ制度に基づいてゲーム理論的に組織の設計も変わってくる可能性があるということで、組織設計が変わると当然ビジネスフローも変わってくるということになるかなと思っています。

一つ例を挙げますと、監査法人のグローバルファームは、ブロックチェーンをものすごく研究をしていますので、「なんでそんなにブロックチェーンを研究するんですか？」と、前聞いたことがありますが、やはり監査業務にブロックチェーンというのは非常に有効ですということでした。一度書かれた伝票が改ざんできないというのは監査するにあたって非常に有効だということを言っていました。ただ、私がそこで言ったのは、「いやいや、そうは言っても、伝票に書くまで、あとERP に流すまでに改ざんがされたらどうするんですか？」ということを申し上げましたが、「そこは論点としてありますね」と。それをもっともっとさかのぼっていくと、部品を作るところから、メーカーが部品を買って、物を作って、それが在庫になって、消費者に流れるという、この一連の流れがブロックチェーン、あと IoT を使うと全てトレースできるようになる世界がやってくるということで、企業の行動そのものを変えてしまうこともあるのかなと考えております。

あるいはリコールなんかが発生したときに、すぐ部品までさかのぼることができるということで、企業行動、プロセスが変わるということで、実際メーカーの人とかと話していたら、「仮に自動車メー

カーが部品のトレーサビリティを求めてきたら、ブロックチェーンで証明書を出さないといけない時代が来るかもしれませんね」ということも言っていましたので、そういう意味で透明性というのがブロックチェーンを使って大きく変わるところかなと思いました。

佐々木：

ブロックチェーン、あるいはむしろビットコインと言ったほうがいいのかもしれませんけれど、その大きな特徴に匿名性が高いということがあったと思うのですが、匿名性と透明性の関係については、どういうふうにお考えでしょうか。

竹田：

匿名性に関しては、これはビジネス的観点から申しますと、銀行は本人確認済みの口座での取引を前提としていますので、あまりここで議論はしたくないというところです。はい。

佐々木：

むしろどういうシステムを組むかが問題で、匿名性の高いビットコインのようなシステムだけでなく、ブロックチェーンを使って組まれるシステムはさまざまあるという、そういう理解でよろしいでしょうか。

竹田：

匿名性の究極は現金なので、その現金がどうなりますかっていう議論にもつながっていくと思いますけども。

佐々木：

ありがとうございます。

そうしましたら、次は前園さんに。「ひと、もの、ことの証明業務」、このあたりのところが変わるということについて、ご説明いただけますか。

前園：

もう今、竹田様に半分以上、７割ぐらい言っていただいたと思うんですけど、まさにそのバリューチェーン今でもあるわけですけども、バリューチェーンに対してどういうブロックチェーンの要素技術を使うことによって、業務が効率化するか。これはネットワークにつながるものが増えるんですね。

例えば、センサー一つずつに付くとか、ネットワークバンドが広くなったときに人が本当にどこで何をしているかみたいな情報まで、取れるんです。実際、携帯で皆さんが何をしているのかって

いうのは取れちゃっていますんで。それに対してプロセス、ビジネスサイドからすると皆さんに何を還元するかということと、それがやっぱり証明、いいことの証明もありますし悪いことの証明も含めて、つながっている情報をどう使うかというのがこれからの社会インフラ、特に、そこに法律ですとか実際の企業の付加価値があるわけですから、それをどうコンソーシアムの中で、いわゆる透明性の高いエコシステムを作っていけるかということで、いろんなものの、例えば、私がどこ出身で血液型が何型でなんていうのは、ある特定のところには個々に入っているわけですけども、それを逆に使うことによって保険のサービスをうまく受けられるようになるのかもしれませんし、もし事故に遭ったときには、私はすぐにその場で血液を供給される可能性もあるわけですね。

ですから、現実社会でのいろんな利用シーンがあるんですけれども、その証明というのが、ブロックチェーンの要素技術をきちっと使えるようになればいろんなビジネスで使えるようになるというふうに私は考えております。

佐々木：

ありがとうございます。

宝木さんは、金融から始まって、次は情報通信とか交通とか、医療。このあたりはいかがでしょうか。

宝木：

単純にここ５年、10年考えると、とにかく熱心な業界がこれですね。火がついていると言ってもいいです。金融はすでに起きているし、この７月１日からビットコインに変えても課税されなくなりました。まだちょっと現象が見えていないのですけれど、皆さん気軽に買えるんですね。８％取られないので。これはどうなるか。非常に気になりますし、とにかく変革が続くと。ただその後、やはりやる気のある業界は、情報通信サービス、これはなぜかというと全分野で使われますので。

それから今、火が付いているコネクテッドカーを含めた交通ですね。あるいは、いろいろ問題になっていますSuicaの情報を取るとか、駅で取るとかいう、そういう交通、鉄道の分野もいろいろあるということで。ここら辺はいわゆるアカウンタビリティと透明性とか処理の公平性とかですね、いろいろ要求されます。

医療は、ご紹介したように、レジリエントの災害時には最もこういう情報が必要なのですが、残念ながら業界が熱心じゃないと思います。なぜかというと、火が付いてないというか、一応は付いてるようなのですが、カルテの共有化とかですね。ただ、日本の医療制度って、たぶん世界でもトップクラスの幸せな制度ですよね。そんなに熱心にならない可能性があるということで、本当は進んで欲しいのですが、これは医療関係者から「いや、そうではない」とぜひ言っていただきたいという意味でも、医療は遅いのではないかというのをあえて挙げたいと思います。

佐々木：

では、久保田さんのお答えは金融決済ということですが、このあたりについてお話しいただけますか。

久保田：

今もご指摘いただいたように、すでに金融決済では動きがあり、例えば日銀はFinTechセンターをつくって仮想通貨やブロックチェーン等を盛んに研究しています。金融庁や経済産業省ではFinTech振興策を様々に打ち出しています。これは各国どこでも同様で、様々な産業振興策を講じています。金融決済の身近な動きの中で、私が特に注目する点は、まず外国送金の手数料がブロックチェーンの活用で劇的に安くなる可能性です。一方、金融決済に関して、仮に先ほどのAppleやGoogleなどが参入すると、銀行業が今まで高いお金をかけて巨大なコンピュータを維持してきたのに、急に水道官の管理屋さんみたいに安いお金でインフラを売るあまりもうからない業種になってしまう可能性があります。すると、銀行が既存の決済情報に如何なる付加価値を付けて生き残るのか。この辺りに関心があります。、その他、法律的には先ほどの域外適用とか、国内法整備が重要課題です。何度か話に出ました資金決済法について、既に完成した法律があるかのように思われるかもしれませんが、仮想通貨の私法上の位置づけは今後十年間をかけて整備する予定であるなど、環境変化に応じて「走りながら考える」状況にあります。これは各国とも同様です。

佐々木：

ありがとうございます。

今の久保田さんの発言、私はとても興味深くうかがわせていただきました。特に銀行業の話ですね。三井住友さんもそうかもしれませんが、日本中、世界中のさまざまな銀行がいま一生懸命FinTechの開発に血眼になっているわけですが、これは下手をすると自分で自分の首を絞めることになりかねないのではないかという、ちょっと意地の悪い思いもしないでもありません。そのあたりについてお伺いしてもいいでしょうか。竹田さんどう思われますか。差し支えない範囲でおっしゃっていただければと思います。

竹田：

おっしゃるとおりだと思いますので、今の私の仕事はイノベーションの通じて既存の銀行業務を変えることだと考えています。このままだとまずいよねというのは共通の認識で、経営陣まで理解していますので、少しずつかもしれないですけども、金融においてもしっかりイノベーションを起こして、業態を変えていくということが必要なのだろうなと思っています。

佐々木：

金融業はこれからどういう方向に変わっていくんでしょうか。つまり、基本的には今までの日本、いや日本に限らずどこでも、銀行というものは基本的には預金を集めて、お金を貸して、利益を得るというのが基本的な業務ですよね。今は確かにそもそもお金を貸しても借り手がいないと言う状況もあります。また、金融テクノロジーが発達していろいろなテクノロジーを使って利益を出す機会が逆に増えて来る場合もあります。こういう状況の中で、銀行はこれからどういう仕事をしてくのかというようなことは、どうお考えですか。

竹田：

質問２でお答えしようかと思ったんですけど、先に申し上げますと、佐々木先生のお話の中で、「業務範囲規制があって、銀行ってやれることが決まっていますよね」という話があったかと思うんですが、確かに銀行法上は銀行ができることというのは限定列挙されていましたけども、この４月１日から銀行法が改正されておりまして、金融庁の認可を取れば、銀行法上限定列挙で書かれていない業務はできる、あるいはその企業を買収できるということに変わっております。

従いまして、商流と金流が分かれていて、このままいったらどうなるんですかというご指摘あったんですけども、一応法律上認められて、金融庁が許可すればECモールの買収もできるようになっておりますので、それはこの４月から法律が変わっておりますので、われわれとしてはそれをどう生かすかというところを考えていかないといけないところです。

では、銀行業ってどう変わっていくんですかという佐々木先生のご質問ですけれども、あと、久保田先生のスライドの中にプラットフォーマー対銀行というコメントがありましたけども、これまではそうでしたということだと思うんですが、できればわれわれもプラットフォーマーになりたいというふうに思っています。ですので、金融機関同士の戦いというよりは、今はもう、これからGoogleだったりFacebookだったりAmazonというところと同じ列でわれわれも戦っていかないといけないなと思っています。そこで得られる情報を生かしてどうビジネスしていくかということです。預金、貸金だけではなくて情報を生かしたビジネスモデルを作るというのが、銀行、金融機関としてのイノベーションの方向性かなと思っています。

佐々木：

このあたりの論点はいろいろとあると思うのですが、宝木さんのお話にあった医療がちょっと縮まり気味だということですが。SAPさんはいろんな業種のお手伝いをしていると伺っておりますが、アメリカの医療は完全にビジネス化しておりますが、御社の場合医療との関わりというのはおありですか。

前園：

そうですね。もちろん、例えば情報を取るという観点で申し上げるんですけども、アンダーアーマーさんは、もともとアディダスやナイキに次ぐスポーツウェアの会社さんで、もともと、コンシューマーに向けてプロダクトアウトをしてビジネスをしていました。今、彼らとわれわれがやってるコ・イノベーションの中で、個人個人のウエラブル端末、デバイスなどから様々な情報を吸い上げてたりしていますが、アンダーアーマーさんは、実に１億6,000万人の情報をすでに持たれています。

彼らがそれを使ってどうするかというのが、まさに次のステップになるんですけども、一つは医療への還元ということを彼らは考えられています。それに近しいものとしてわれわれも実は、社員が参加するフィットネスプログラムを展開しています。Fitbitなどのバンドを付けて、世界中で参加している社員が１日にどれだけ歩いているかみたいな情報を集めています。そういう仕組み自体がすでに動いているのをお客様に見せるということは非常に重要で、そこから損害保険会社や生命保険会社などと次のサービス展開の話をできるようになってきますし、現時点では医療側から入ってくるというよりも、どちらかというとデバイスから上がってくる健康情報みたいなものを、医療保険ですとか、医療現場そのものでどう生かすかというような、ビジネス展開やPOCみたいなものを世界中で幾つも検証している状況でございます。

佐々木：

実は、これに関しては、後で情報をどこまで使っていいのかという話と結び付けたいと思いますので、差し当たっては、この件はここで終わらせていただきます。次の質問に移らせていただいてよろしいでしょうか。

【質問２】：ブロックチェーンは既存の社会における規制のあり方にどのような影響を与えると思いますか？

これもちょっと雑ぱくとした質問に見えるかもしれませんけれども、ブロックチェーンというのは､基本的にはできるだけ中央集権的な統制を廃していきましょうという考え方であります。ただ､そういう形で分権化を進めていくと、既存の社会との間でいろいろなコンフリクトが起きたりする可能性もあります。あるいは現在ある規制の在り方に対して、何か影響が及ぶ可能性もあります。逆にこういう規制は邪魔だというようなお話でもけっこうですが、とりわけ規制との関係についてちょっとご意見を書いていただけたらと思います。

佐々木：

まず久保田さんのほうからお願いできますか。

久保田：

私は、「今は育成、将来は規制」と書きました。ブロックチェーン取引の典型例である仮想通貨を法的にみると光と影の両面があります。取引が発展段階にあれば光の部分（例：信頼できる安価な取引）が目立ちますが、成熟段階に入ると影の部分（例：資産が全て仮想通貨ならば差押えが困難、プラットフォーマーによる仮想通貨の寡占化に伴う銀行業の衰退）が相対的に拡大します。従って、発展段階の今は、何か問題が起きる可能性があったとしても今つぶしてしまうとビジネスが発展しないので、「レギュレータリー・サンドボックス」でビジネスを育成し、規制の効果を実験しながら前に進むわけです。イギリス発祥の規制方法ですが、取りあえず「規制のお砂場」でもって規制を緩和して当事者に自由に取引させてみて、不都合が生じれば規制を加える一方、うまくいくようならば、自由化するわけです。

しかし、取引が拡大すると今度は影の部分が目立ってきます。そこで、徐々に規制を強化していき、健全な取引が発展するように努めます。発展段階の今はじっくり見て、でも成熟段階に入り、問題が拡大したら果敢に規制するという方向性が望ましいと思っております。

佐々木：

最初からこんな恐れもある、こんな恐れもあるといった形で、がんじがらめにするのではなくて、とにかくやらせてみよう。問題が起きたら考えましょうと言うことですね。

ところで、今はいろいろな混乱が生じたとしても、どれくらいたつとブロックチェーンを含むシステムは安定的になってくるのでしょうか。

久保田：

金融決済に関して言うと、既に規制を強化すべき分野もあります。例えば、闇ウェブを利用した犯罪対策やマネロン対策です。それ以外の分野でも意外と早く規制局面が来る可能性があります。例えば、外貨送金が日本ではまだ高いですが、如何なる手段によっても 5,000 円はかかっていた時から PayPal 等が参入して劇的に安くなるまでの時間、あるいは金融決済以外でも民泊においてAirbnb の参入から民泊新法の成立に至るまで、従来に比べるとかなり早かったと思いませんか？すると、ブロックチェーンでもし新しいサービスが登場すれば、それが日本で急速に拡大し、規制局面をもたらす可能性があります。

佐々木：

国境を越えた取引になると、規制するといっても国際協調でもしないとなかなかうまくいかないと思いますが、そのあたりはどうお考えですか。

久保田：

そうですね。これも法的には大変興味深いテーマです。国際的な金融決済、すなわち国際金融の世界では、いわゆる法的拘束力のある法律ではなく、法的拘束力のないソフトローという形（例：G 20 合意）で、最初に国際統一方針が決められると、国際機関や各国当局がそれぞれ取り締まりにかかります。例えば、マネーロンダリングとか、BIS 規制とか、みんなそうです。国際的な規制の方向性のかじ取りを巡っては、従来はアメリカのリーダーシップが際立っていましたが、中国の台頭もあり、日本が如何なるリーダーシップをとっていくかが課題です。

佐々木：

これについては、例えば国際会計基準や税制などのコンバージェンスの話などと同様に、今後日本がこれからどういうところで、どういうリーダーシップを取るのかということが、一つのポイントなのでしょうか。

久保田：

日本人ってどうしても空気を読んでしまう面があり、やはり国際会議などに出ますと、日本人というだけでサルを見ているみたいな感じで接せられることも多いのですが、そこでいかに自己主張できるか、メンタルを強くできるかというのは課題かなと思います。

佐々木：

それでは次に、宝木さん、ご説明いただけますか。

宝木：

ブロックチェーンがもたらす情報技術は、大きく三つの特徴があって、匿名性と、それから透明性。オープンデータから透明性は実現しやすい。匿名性はできます。それから、もう一つの大きな特徴は、アカウンタビリティ。やったことの責任は取らせることができるのですね、ゼロ知識で。名前はばれないのだけれど、現金は引かれてしまうとかですね、罰金取られるとか。そういう技術はたぶん共通です。問題はこの監視ですね。監査を入れることは可能でして、そのうえでこれが３通りあるのではないかと。

一つは「オセアニア」というジョージ・オーウェルが描いた世界の、ビッグブラザーの世界で、社会の回し方はブロックチェーンで非常に効率よく回す。ただし監視はきついと。

それから二つ目は「イースタシア」というジョージ・オーウェルが言っているやつですが、これはたぶん夜警国家であって、かつ自由という、どっちかというとわれわれが目指したいような、ちょっと監視も非常に妥当な世界。

三つ目の「ユーラシア」ですけれども、ジョージ・オーウェルは、一応「統制が取れた地域」と

言っているんですが、僕は、これはひょっとしたら統制が取れずに、無政府、無秩序なエリアがまだ、例えば10年後、より進んでいるのではないかと。

そういうところで、たぶん、貨幣というのは、おそらくビットコインみたいなのがさんざん使われたあげく散々になっているかと。無政府状態の国で貨幣というのはそういうのがたぶん有効ですので。そういうあたりで、ちょっと監査機能の強弱という観点で、先ほど中国とかアメリカとかの話が出ましたけども、そういう特徴づいた形で進んでいくのではないかというふうに思っております。

佐々木：

今、規制という話が出ました。国家との関係ということで今の三つの類型の話が出たのだと思います。先ほどの前園さんのほうから、例えばさまざまの健康情報を蓄積して、それをビジネスに役立てたいというようなお話もありましたが、ジョージ・オーウェルが考えているようなオセアニアは、国家が中央集権的に国民を管理するという世界でしょうが、今後はむしろ巨大企業が、例えばGoogleなどが、情報をたくさん持ってしまって、それが情報管理するというような世界が生まれる恐れはないのでしょうか。

宝木：

企業の場合は政府ではなくて、やはり一応、企業には政府が上にあると考えます。民主的な世界でのGoogleさんということになりますと、何らかの選挙によって統制が効きますので、これはイースタニア的な世界、いわゆる自由な中で発展するモデルとして捉えたいと思います。ただ、ある程度は規制を入れないといけないのですけれども、ビッグブラザーの世界ではないような、全員が納得できる形というのをぜひ目指していきたいというふうに思っております。

佐々木：

つまり、国家が情報を持つのと、たとえ大きな会社であろうとも民間企業が情報を持つのでは、やはり違うのだという、そういうことですね。

宝木：

違います。そういう意味で、先ほど申し上げた夜警国家としての位置付けがあると、われわれはちょっと自由な息ができるのではないかなと。

久保田：

法学部所属なので国家寄りの見方かもしれませんが、民間企業に任せておけば、ちゃんとやってくれるという考え方は、やや楽観論のような気もしますが、如何でしょうか？例えばGoogleに独

裁者が出現し、「アメリカだと取り締まりが厳しいから、じゃあアメリカの管轄の及ばない所を根城にして、俺が国家のように、事実上世界を支配してやる」ってやったらできちゃうんじゃないですか。

宝木：

それをやると、今度 Google がいる場所がユーラシアになるかもしれないですよね。民衆の反乱ですかね。どこかでしっぺ返しを食らうと思いますね、金正日みたいなのがトップになったら。だから、この三つのどこかに行くんではないかと、私のちょっと荒っぽい、ちょっとイメージです。

佐々木：

ご質問があったら、私が質問するだけでなく、どんどんご意見を言ってください。では前園さんの「トライアル特例」というのは、どういうことでしょうか。

前園：

まさに、今日も新聞に出ていましたが、このレギュラトリー･サンドボックス的なモデルこそが、われわれ自身がいくつもの企業と一緒に多数こなしているトライアルそのものですし。例えば、日本でそういったものをやるとすると、国主導でないとまとまりにくいとか、戦略特区みたいなところをもう少し開放して、例えばビットコインをベースにした金融決済でもいいですし、医療でもいいですし。ちょっと小さい単位の枠組で試してみないと、われわれ自身も安心、納得できないですし、当然法律とかも整備できないのだと思います。あと例えば、EU なんかでは当然 EU 統一基準の中でできることをやられますよね。

ちょっとこれは我々が直接ではないですけど、エストニアなどの小国、われわれがマイナンバーのモデルにした国ですけども、国が個人の大概の情報を管理しています。ただ、それは当然トレードオフがあるわけですけども、利便性ですとかという意味では、非常に最先端のシステム事例として取り上げられています。残念ながらまだブロックチェーンの技術ではないですけども、技術的には今後、十分に転用できるエリアではないんじゃないかなと思って、今回は「トライアル特例」というふうに書かせていただきました。

佐々木：

現在、日本で「特区」がたくさん作られておりますが、それはまさにそういう思想でつくられているのだろうと思います。ただ、私などかは特区というと、とても疑問に思うのは、実は、普通であればまさに実験をする場所ですから、それに適した典型的な社会構造を持っているところでなければいけないわけですけども、現実の特区は、実は一番反対の少ないところで作られる傾向にあると思います。例えば、Uber などをたぶん東京でやると言ったら、タクシー会社が潰しにかかる

と思うんですね。それに対して、ほとんどタクシー会社もないような過疎地域であれば、Uber を許容する特区をつくったとしても、むしろみんな賛成すると思います。しかし、そこで実験しても―これも意地の悪い質問かもしれませんが―、あまり意味がないのではないかという気もします。この点はいかがでしょうか。

前園：

日本でも過疎地でまさに Uber が求められていたという問題がそこにあると思うんですけども、ある一定のレベルが必要だとと思います。そのレベルを上げていくときに、コンソーシアムみたいなものが出来上がり、例えば、ヨーロッパとかでみられるのは、レベルが上がるときには必ず行政、有識者、法律家の方々が入って、一緒に育てるというアプローチも取られていると思います。

日本の場合は、場所や時限に資金がついて、そこで「やれ」、試せ的な話がほとんどで、結果よかろうがが悪かろうが、なんかやるかやらないかの０・１で、予算ありきのモデルなので、もう少し余裕のある仕組み、育てる的な、フェージングみたいなものを、行政がガイドするのか業界団体としてナビゲートするのかというのはあると思うんですけど、そういう何か協調性のあるやり方というのは、海外ではよく取られているのかなと思います。

佐々木：

竹田さんのお答えに行く前に、今の件をもう少し深めたいと思います。前園さんはまさに SAP というグローバル企業の経験の中で、そういうトライアルということをお考えになっていたわけです。そういうご経験を踏まえて、今おっしゃったように、日本に目を転じてみると、日本はどちらかというとトライアルではなくて、みんなが言うからやりましょうとか、業界団体が言うからやりましょうというような、そういう風土があると言うことだと思います。私も同感なんですが、そういうことで日本企業はいいのでしょうか。あるいは、やはりここは変わらなければいけないというようなことがあるのか、ということですね。ここだけの話ということで（笑）、日本企業のご経験がおありの宝木さんや竹田さんなどに、外資系との風土の違いみたいなものから、こういう問題にどうアプローチしていくべきなのかなど､お話しいただけるとありがたいと思います｡いかがでしょうか。

宝木：

仕事上、いろいろ外資系、IT 企業とはですね、結構、しょっちゅう交流しております。佐々木先生もたぶんそうですけれども。やはり IT についてはですね、IT リテラシーというのですかね。外資系の方は非常にレベルが高い。なぜかというと、特に米国は、いわゆる境界、国境なしに世界中の優秀な人を集めて、分厚い仕様書マニュアルを、たぶん日本人が作るより２倍以上速く作るのではないですかね。IT には向いています、おそらく、IT 開発。それからリテラシー、特にセキュ

リティに関する感度というかトラウマというか、ヨーロッパ、米国のほうがきついと思いますね。過去、痛い目に遭っているというのもあるのですけれど。そういう意味で、動機とそれから環境、優れています。

ただ、それでいて日本は絶対勝てないかというと、実はそうでもなくて、意外にしっかりやっています。マニュアルの厚さは、たぶん 10 センチと 3 センチぐらいの差があるのですが、内容がだいたい濃いですよね。という感覚もあって、しっかりやるという精神はあるということで、ものづくりに対する魂というのは、なにか違うなということで、そういうのが生かされるようには願っているし、それが生かされている分野も確かにございますので。今のところは、6 対 4 ぐらいで負けている、全体的に負けているかもしれない。特に、IT 関連の金融系はですね。ちょっと技術的には、いずれ盛り上がる余地は十分あるのかなというふうに考えております。

佐々木：

よろしかったら、前園さんも何かあれば。

前園：

外資系ですけど私も日本人ですので、当然日本の企業のこともいろいろご支援させていただいておりますし。トヨタさんは製造業ですけども、トヨタ式生産方式を海外で展開されて成功されていたり。あとスズキ自動車さんとかも、今インドに出て行ってマーケットも取られているということで。やっぱり日本はモノをきちっと作って、そのモノ作りの価値が評価されるという仕組みにおいては非常に得意ですよね。SAP はドイツが本社ですので、ドイツと日本のモノ作りという観点のでは、政府間でも非常にいい関係です。

先日 CeBIT というも国際イベントがハノーバーでありまして、安倍さんがわれわれのブースに来られてわれわれのブースを見学されて帰られて、その後に、インダストリー 4.0 文脈の中で、ドイツと日本の中でモノ作りと IoT、その先には FinTech であったりブロックチェーンという技術をどうやっていこうかということなどが議論されだしたのも、日本の企業のいいところというのを、どうグローバルに展開していくかということこそが、これからの日本企業の課題だと思っています。

佐々木：

竹田さんいかがですか。感想でも結構ですけども。

竹田：

たぶん金融の場合は、またちょっと特殊なところはあるかと思っています。世界中どこに行っても規制の対象になっているので、自由に活動するというのがなかなかしにくいということで、まず試してみるというカルチャー、外資系の場合なんかはどんどん試してみたり、自由にグローバルに

やられているとは思うんですけども、そこで規制で行動に制限がかけられてるというところで、そこが変わるとちょっとカルチャーも変わってくるのかなとは思います。

アメリカの金融機関と日本の金融機関やり方が違うとすると、日本の金融機関はアメリカの金融機関に比べて、アメリカの金融機関の場合は技術者を中に囲っているケースが多くて、技術者の比率が非常に高いというふうに言われているんですけども、日本の場合はなんで低いかというと、そこはベンダーさんに任せているからでありまして、ベンダーさんと密にリレーションを取っていることで新しいことはベンダーさんにやっていただいて、それを最終的に製品化するときは一緒にやるというような方法に、日本の金融機関の場合は長けているのかなと思います。内製しているか外製しているかというとこの違いかなとは思いますが、トータルでシステムに関わっている人ということを考えると、実はあんまり比率的には変わらない可能性があるというふうに思います。

佐々木：

おっしゃるように、金融はどこの国でも規制産業ですからね。だからそういう点では先ほどの医療などのほうが、典型的かもしれませんね。医療の場合、日本は典型的な規制産業ですが、アメリカなどは非規制産業です。そちらのほうがより問題をはらんでいるのかもしれませんね。

それでは、竹田さんの銀行のことについてご説明いただけますか。

竹田：

そうですね。今申し上げたように、金融機関世界中どこに行っても規制がかかるということと、国内におきましても、実は銀行法だけではなくていろんな規制、ビジネスやる上ではかかってきておりますので、若干ここには控えめに書かせていただいておりまして、当たり障りのない業務範囲規制というところで一応書いています。

業務範囲規制は金融庁さんの後押しもありまして、先ほど申し上げたように銀行法は改正されてどんどん規制は緩和してくれている方向にありますので、これをうまく使いたいなとは思いますけども、やはり世の中のスピード、コンペティターとのスピードという観点では規制がかけられているという点でスピード感には劣るというのは否めませんので、新しいことをどんどんやっていくという意味ではやりやすい環境にしていただければいいなと思います。

先ほどレギュラトリー･サンドボックスの話も出ましたけども、２月に私、UK 行ってきてレギュラトリー・サンドボックスって、実際金融でどう使われているかのかなというのは調査してきました。そのうち日本でも導入されるんだろうなと思って２月に見に行ったんですけども､意外と早く、国としてもレギュラトリー・サンドボックスという言葉を初めて打ち出しましたので、この後の設計ですね。使い勝手がいいように設計してほしいなという希望はあります。

UK の場合は、特に金融の場合は金融立国を目指しているというところもありますので、国としてもレギュラトリー・サンドボックスを率先して使うように言っていますけども、日本でどれくら

い使い勝手のいいものをつくってくれるかというのはこれから期待したいなと思っています。

佐々木：

そうですね、イギリスはある意味で金融とそれ以外の産業の生産性の格差が、ポンドの実感的な価値への違和感のようなものを生み出しているのかも知れませんね。そういう点では、確かに日本にそのままそれを移植するというのも、難しい部分があるのかもしれません。ただ、そうは言ってもやはりできるだけ規制は緩やかにしていったほうがいいのかもしれません。

このあたりで、何かご意見、言い足りないこととなどがございましたら、お話いただけたらと思うのですが。久保田さんどうですか。

久保田：

そうですね。法的なところから多少補足しますと、先ほど特区の話が少し出たので、例として民泊についてお話しましょう。オリンピックに向けてホテルが足りないので皆さんが住んでるご自宅を貸してあげましょうという発想の民泊ですね。民泊特区法という法律ができて、大田区とかが開始したけれども、あまりに要件がきつくて参入がなかなか進みません。あるいは、政府がようやく重い腰を上げて民泊法案を作りました。しかし、年間営業日数が半年しかできませんし、イベントのときに来てもらうイベント民泊は年に１回しかやってはいけないとか、厳しい縛りがあります。このように、既存の旅館業者との利害調整過程で、ビジネスの自由度が非常に狭められてしまうわけです。やや脱線しますが、銀行の業務範囲規制について、IT 業界への出資が最近可能になった背景にはアメリカで規制緩和した影響があり、日本国内では長らく銀行の他業進出（例:不動産業）は進出先業界の反発で難しい状況にありました。

ですので、政府がなかなかできないのは、利害関係のしがらみと、法律が許容する自由度があまりに小さいという面があります。その辺をある程度変えるか､あるいはレギュラトリー･サンドボックスのような中間的な制度を作って、自由度の大きい取引を試行的にやらせてしまうとか、そういう工夫が必要なのかなと思いました。

佐々木：

フロアから来ている質問がございます。その中で、実は量子コンピュータの話へのご関心のある方がかなりいらっしゃるのですね。それぞれの質問のニュアンスは若干違うのですが。

ご存じの方も多いかと思いますけど、量子コンピュータというのは、今のコンピュータとは全く違う原理で動くコンピュータです。要するに、量子力学の重ね合わせの原理を適用して計算をしていくわけです。非常に超高速の計算ができるということが期待されています。理論的には、ずいぶん昔から言われていたわけですけども、だんだんと最近になって技術的にも射程内に入ってきているように見える部分もあります。ただ、これが出てくると、暗号等々もいろいろ影響をこうむる可

能性があるなど、様々な問題があるかと思います。これについては宝木さんに、量子コンピュータの可能性や、それがもし実現したらどうなるか、などといったことをご説明いただけませんか。

宝木：

量子コンピュータの概念自体はだいぶ前に、何十年前に出ているのですが、量子暗号と量子コンピュータの二つありまして、量子コンピュータというのは、重ね合わせの原理で、同時にいろんな処理をやってしまうという機能などがあって、例えば、現在の世界中のコンピュータを集めたよりも、何億倍もあるいは何千億倍も早く素因数分解ができてしまうとかですね、そういう方法があります。

それで二つあってですね、ゲート法とアニーリング法と二つありまして、ゲート法の量子コンピュータの物理現象は成立していますが、ただ、しゃぼん玉のように一瞬にして消えてしまうというのがありまして、全然安定しないんですね。常温超伝導みたいに、できる、できると言ってできないと。ただ、ハードウェアがなんらかの物理的な組み合わせでできてしまった場合は、安定してゲート法でコンピュータができると。少しでも長く続いてしまうとなれば、もう世界中のRSA暗号とかSSLとかいろんな、いわゆる古いタイプの公開鍵暗号は解ける。ビットコインで使っている楕円曲線暗号も解けます。

従って、公開鍵暗号と秘密暗号のペアは簡単に偽造できると。ただし、ビットコインは幸いなことに、ハッシュ関数という関数、これはゲート法のコンピュータができても、ハッシュ関数を破るソフトって全然誰も思い付いてないのですね。ないという証明はないですけども。ということで、過去の履歴の偽造は相当難しいと言われていますので、過去の履歴の該当箇所を選りすぐりしてすべて見つけ、都合のよいようにすべてをいっぺんに改ざんするというような破局には至らないと。ただ、ビットコインそのものはクラッシュしていくだろうと思います。それが一つ。従って、ゲート法の量子コンピュータは、明日できてもおかしくないし、100年たってもできないかもしれないという状況です。

もう一つは、アニーリングというハードウェアの方式があります。これは焼きなまし法といいます。これを使うと巡回サラリーマン問題とかですね、ある種の問題を解けるというのが分かっていますが、素因数分解を本当に解けるというソフトが見つかっていないのですけども、こっちのほうがむしろ見つかるのではないかという意見をいろんな人から聞いています。従って、ソフトが見つかってしまえば、かなり危ないですね。

従って、アニーリング法というのは一部製品化されたし、Googleなんかも使っていますけれども、これも要注意ということで、早晩、いわゆるプレ量子コンピュータ型の暗号は、
変えたほうがいいと思います。

そういうことで、ポストコンピュータ型の暗号方式というのがございますので、いろんな別の原理を使った公開鍵暗号はそれに置き換えるという方策をしないといけなくて、これはちょっと暗号

研究者の責任かなと。私も含めてですね。当局にどんどん言っていかないと、いざというとき非常に大きな世界的影響を与える事態になりますので。そういう問題があるということで、あまりのんびりしていてはいけないなという感じを持っています。

佐々木：

確かに、アニーリング法は、いわゆる制約条件付きの最適化問題を解くことに特化した方法論だというふうに理解しておりますけれども、今のお話ですと、うまくプログラムを組めば、素因数分解等々もできてしまうかもしれないということですね。そうすると、今の暗号システムというのはかなり危機に陥る可能性もあるかもしれません。アニーリングコンピュータ自体はもう動き出しているわけですね。カナダのベンチャー企業が実際に作ったようです。

ただ、そうなると、一つには、まさに宝木さんのご専門の暗号についても、これから技術の問題としては非常に重要になってくると思います。このあたりについて、一つは日本の暗号研究はどういう状況なのかということ、それから世界的に見たときに、そういう技術の急速な進歩に対してちゃんと対応ができているのか、このあたりはいかがなんでしょうか。

宝木：

基本的に日本人の性質かどうか知らないのですけども、数学というのはかなり強いのですね。江戸時代から、関孝和あたりからかなり強くて、現代も暗号研究をやっている人のレベルは世界レベルで、ダルムシュタット工科大の公開鍵暗号の解読コンテストでも、過去何回も続けて優勝しているとか、結構いい線を行っています。改良型センスはものすごくあります。ただし最初の改革的、大変革的な定理とかアイデアというのは意外に海外から出るのですけれども、それを受けた後のチェンジ、改良、これは素晴らしいものがあるということで、それほど悪くないです。

あと、公開鍵暗号で、ポストクオンタムの暗号としても、いろんな方式があるので、それについても鋭意世界レベルで研究開発してかなり実用に近いものもございます。日本人が頑張っていると言えます。

佐々木：

このフォーラムは、どちらかというとビジネスサイドでブロックチェーン技術等々をどう使うかといったような問題や、それがもたらす社会の問題等々を考えているわけです。これについては、三井住友さんもいろいろ頑張っておられるし、SAP さんも頑張っておられるということで、それぞれのビジネスサイドでは皆さん頑張っておられますが、例えば、しっかりとした暗号技術の確立というのは、個々のビジネスの問題というよりも、むしろある意味で社会全体の共有の財産の確立の問題だという部分がございます。そうすると、これについてはむしろ国家プロジェクトとして必死になってやらなければいけないものかもしれませんね。そういった点について、日本政府の姿勢

は、たとえばアメリカ政府と比べてどうなのでしょうか。

宝木：

最近こそ増えていましたが、つい数年前までは国の予算は非常にお粗末で、欧米に比べ何分の１以下でしたね。いわゆる学術予算ですね。産業予算というのは別にあるのですけれども、暗号の基礎研究はやはり学術系、文科省系から出るべきものですが、これはいまだに不十分と私は思っています。

これは、予算は提案するのですけれども、なぜか先生方の投票数が少なかったりする。今年もです。ということで、実はいろんな文化系の先生も含め、そういう審査をする場があるので、そういうところでぜひ大事だというふうに言っていただくことですね。やはり分野の人口規模が増えますと、いい人が来ますということですね。

今のところ、暗号研究者は、残念ながら油断すると高学歴プアになります。５年ぐらいある期間いて、終わったらもうちゃんとした給料で働ける場所が見つからないとか、まだそういう状況ですので。そういう面でも、体制といいますか、サステイナブルな、継続可能な大規模な研究の場はつくるべきじゃないかなというふうに思っています。ヨーロッパはヨーロッパで、「Horizon 2020」でしたか、すごい予算を組んでいますし、米国はそれなりに出ていますので、そういう意味では、ぜひ、いいご質問をいただいたので、そこはぜひ清き１票をいざというとき入れていただければと思います。

佐々木：

そうですね。暗号が崩れてしまうわけです。つまり、ある意味どんなシステムも丸裸にされてしまうことになりますね。むしろ、そこへの信頼性をベースにして、はじめて今の FinTech やブロックチェーンはあるということですね。そうなると、暗号に関する不安というのは、ちょっと危機的なことかもしれません。皆さん、声を大にして、もっと暗号研究にお金を割きましょう、ということを政府に対しても言ったほうがいいようですね。

そうしましたら、質問に戻りまして、質問３にお答え頂きたいと思います。これは、今日のシンポジウムをある程度踏まえながら、10 年後の日本と世界がどんなふうになっていると思いますかという質問です。夢のような話でもいいですし、あるいは逆に、非常に深刻なこういう問題を起きているかもしれない、というようなことでもよろしいので、一つ特に代表的に気にされていることを書いていただけないでしょうか。

【質問３】：10 年後の日本と世界はどのようになっていると思いますか？

ある意味で一番奥の深い回答につながりそうな、竹田さんの「分からない」というのは、これは

いかがでしょうか。

竹田：

すみません、分からないんです。私の部ができたのは１年半ぐらい前なんですけども、１年半前にブロックチェーンの研究をやっていたかというと、やっていなかったと思うんですね。今は、AIとか力を入れてやっていますけども、その頃「AIって何？」っていう感じだったと思いますので、この１年半で様変わりしています。世の中のスピードは非常に速いので、10年先のことと言われますと、正直分からないと。ベンチャー企業の社長さんなんかに話を聞きますと、「３年先のことなんて分からない」と言われます。「３年先のことを決めていたら駄目だ」というふうにベンチャーの方々はおっしゃいます。世の中どんどん変わっているのに、ゴールを置いて、そこに向かって進むというやり方は、もはやこの時代あまり通用しなくなっているんじゃないかなというのが、イノベーションの片隅にいる私の実感でして、ブロックチェーンもこの先どうなっていくか分かりませんし、量子コンピュータが本当に出てきたら、どういう世界が来るかというのは、妄想はできるかもしれないですけども、やはり実務の観点からは全く分からなくて、本当に日々出てくる新しいものに食らいついて理解していくというところで、正直精いっぱいですので、こういう答えをさせていただきました。

佐々木：

予想どおりに非常に深いお答えだと思います。竹田さんのお話をうかがって、私にとってとても印象的だったのは、「ああ、今は銀行の人がこういうことを考えるんだ」ということでした。これは失礼な言い方かもしれませんが…。

つまり、私たちから見ると、銀行の方というのはとても保守的で、ルールや進路をちゃんと見渡した上で、確実なところを渡っていくというようなイメージがあります。これがちょっと前までの日本の銀行の方のある意味典型的な生き方だったと思うのですが、それが今は走りながら考えるぐらい、テクノロジーの進歩のほうが進んでいるのだということなのですね。だから、そんな先のことなんか考えてられないよというのは、逆に、本当に今現在全力疾走しておられるのだなというふうに思いました。ただ、どうなんでしょうか、竹田さんは、そういう部門におられるからかもしれないですけど、銀行全体もやっぱりそういう流れですか。これもちょっと嫌な質問かもしれませんが。

竹田：

私が異端であるかもしれないというのはそれは確かで、変わった人だねというふうにいろんな人から言われますけども、私、もともと銀行員でございますので、世の中の流れが変わっていくと、銀行員もこういうふうに変わっていくんだなという一つの証かなと思っていますし、銀行全体も、

特に、トップのマネジメントは非常に危機感を持っていますので、分かろうと努力はしていますけども、分かんないというのが印象だと思います。ただ、目先で起こっていることは、ちゃんと食らいついて、それに対して経営として対処していかないといけないなという危機感はトップを含めてありますので、あまり銀行という業態を、われわれはあまり考えないようにしています。一事業者としてビジネスをやっているという感じで、これからもビジネスをやっていくんだろうなと思います。

と言いつつ、たぶん、ゴールを決めてはいけないと申しあげましたが、来週、再来週ぐらいには、中期経営計画という３年の計画が出るという状況です（笑）。今、私が申し上げたことと全く真逆のことを銀行としてはやっているわけでございまして、３年後の出来上がりの世界はあまり当てにならないというふうに私は思っています。

佐々木：

それはどこでもそうですよね。最近は、大学でも中期計画を立てろとか、いろいろ言われて、作文だけはどんどんうまくなっていくのですが、みんな絶対そんなもの実現しないだろうなと思っている、というような状況だろうと思います。非常に率直なお話が伺えて、本当にありがとうございます。

今日の会場にはたぶん学生もかなりいると思うのですが、自分の就職先を考えたときに、もう５年前の職業イメージで就職先は考えないほうがいいということなのかもしれませんね。

竹田：

そうですね。金融志望の方々もいらっしゃるかもしれないですけども、金融というお客様の基盤と、いろんなプラットフォームになり得るポテンシャルは秘めた一企業だと見ていただいたらいいのかなと思いますし、これから戦っていくのはいろんなIT企業さんだというふうに思っていただければと思います。

佐々木：

ありがとうございます。

それでは、前園さんはどうですか。不確かな世界とイノベーション、そのあたりが10年後の未来像だろうということですね。

前園：

そうですね。どういうことが明日起こるかって、分からないわけですね。ただ、テクノロジーが進化をしているというのは皆さん気付いているわけで、例えば、代表的な例で、ご存じの方も多いと思いますけど、2005年のローマ法王の選出のときと2013年の選出のときの比較シーンがよく

Web 検索すると出てきますけども、2013 年はスマホのフラッシュでだらけになっている。要は、2005 年時点ではスマホで撮るということは誰もが思っていなかったことが、たかが 8 年ぐらいで起こっている。要は何かが変わる中で、ただ待っているという、何もしないという選択もありますが、佐々木先生の後半のお話でもありました新しいフィールドを探しに行くという選択、自らが新しいビジネスチャンスであったり、そういったフィールドを作り出すということが必要かと思います。

なぜなら、われわれ日本人は、これから起こる少子高齢化、人口減少、生産労働力減少という世界を一番に経験する中で、それだけは確実に起こることは分かっているわけですから、そういった中で、私はたまたま IT、IoT の世界に近いところで働いていますけれども、それをやっぱり社会にうまく生かせるような仕組みづくりというのに少しでも関われたらなと思って。人類がかつて経験したことのない不確かな世の中になってもイノベーションを自らが起こすことが新たな道を切り開くためにも重要、そういう意味で書かせていただきました。

佐々木：

ありがとうございます。

それでは、宝木さんの「IoT で盛り返す」というお答えは、どういう考え方でしょうか。

宝木：

言葉だけでは非常に陳腐なのですけども、基本的にわれわれ、日本の歴史を見ると、やはり、ちょっといい技術が来たらパッと飛び付いて、いい物を作っていくという特長があります。最初の材料は、外からもらうのだけれど、小さな発明の繰り返しで素晴らしい物を作っていくという歴史があったのです。江戸時代、島津藩により大砲を造ったり、鋳造したり、いろいろあったのです。そして、今、またその時期だと思うのですね。やはり目新しい技術が発表された後、欧米は IT を中心に改良、発展している。日本は従来的な物理制御系の技術の延長上に改良、発展をすることが期待される。

つまり、歴史的に見ると、大きな技術変革はもう一度来るのかなという状況ですね。例えば QC について、米国のクオリティ・コントロールのアイデアを日本に導入した途端、各工場が競って入れて、トヨタのある意味、看板方式までいったと言えます。いわゆるみんなが意見を出してやっていくという、そういう文化があるのですね。器用さとそれを生かす文化を合わせもつ。そういう観点がある。だいたいそういう特性でもってぜひ盛り返していってほしいと思っています。

和魂洋才というよりも、何て言いますかね、そういう特異点があります。たぶん日本はこういう特異点、また、海外は別の特異点があります。今は変革の時代です。10 年後には全然変わっていると思います。これは希望的観測ですけれども、ぜひ IoT でもって、日本のみならず世界がいい方向に行くべきであろうというふうに考えております。

佐々木：

久保田さんは「ソフトローによる米か中の支配権が増大する」ということです。これは、どういうことでしょうか。

久保田：

国際的な規制を見ていると、BIS 規制にせよ、マネロンにせよ、現在は、強国アメリカに対して力負けする欧州・日本の綱引き構造が元々あって、そこに中国が入って影響力を強めています。残念ながら日本はバランサーとして機能できるかもしれませんが、極をつくるほどは強くはないし、今後相対的な影響力は後退し続けるでしょう。でも、商売というのは別に何も覇権国でやる必要もないわけですから、米欧中などのパワーバランスをうまく利用しながら、日本にとって民間企業がうまく潤えば良いのではないか、別に国家が強い必要はないのではないかと思っております。

佐々木：

これについての質問があります。アメリカがある程度､法的な領域でも支配権を持つというのは、ありそうなシナリオだと思うのですが、中国の場合、そもそも法の支配だとかリーガルマインドだとか、そのあたりのベースに疑問の面もありますが、そこが法的な支配権を持つと怖い、ことにならないですかね。

久保田：

おっしゃるとおりですね。ただ、中国も WTO に加盟するなど、国際社会や法化社会の中に次第に組み込まれつつあります。その中で、中国の状況を考えてみると、IT 企業は、むしろ日本よりもずっと勢いがあって強く、少なくとも日本や東南アジアを含めたアジア地域のセンターの一翼を中国は担うことになると考えられるので、今の独裁体制から法化していく可能性は十分あると思いました。

佐々木：

だいぶ時間が迫ってきてしまったのですが、実は、私のほうからさらに一つ、これは書いていただくというよりも、言葉でお話しいただきたいのですが、質問がございます。そもそもなんで私がこういうシンポジウムを考えたのかということですが、確かにまだよく分からないところはあるにしても、ブロックチェーンなどの最近のテクノロジーの発展というのは、非常に驚異的なものがあると思います。

その一方で、早稲田大学は、研究面においても教育面においても、見劣りがする気もいたします。例えば、先ほどの昼の打ち合わせでも、学部にブロックチェーンを教えている講座はありますかというご質問がありましたが、思いつきません。ようやくビジネススクールが今年から三井住友さん

の寄付をいただいて講座を持ったというような状況で、正直言って大学全体で見ると弱いんですね。

それから、法学的な面でもそうかもしれません。ですから、われわれの大学をこれからどうこのあたりの領域で強化すべきなのかということについてお教え頂けたらと思います。もちろん早稲田だけに限らず、こういう最新の技術について、大学と企業はどういう関係を持つべきかというようなことについて、何かサジェスチョンなどがあれば教えていただきたいと思います。これは、むしろ早稲田の外の方に、まずしゃべっていただいたほうがいいんで、竹田さんからお願いできますか。

竹田：

そうですね。早稲田だけというよりは、日本の大学という点で、こういう新しいことがどんどん起こっているというのを、こういった場を通じて分かっていただいて、それをどんどん大学としても講座なり学生の教育の中に取り入れていってほしいなと思います。

逆に、企業側としては、そういう勉強をした学生さんたちは、即戦力として非常に欲しいなと思っているところもあります。特に、日本の場合、理系の学生というのが、今奪い合いになっている状況でありますんで、データサイエンティストですとか、今年なんか滋賀の大学でデータサイエンティスト学科ができたと聞きましたけれども、そういう専門的な将来即最前線で働けるような学生さんたちを育成するような講座をどんどんつくっていっていただけると、企業側にも非常にニーズがありますので、早稲田大学にもそういう外部の講師なんかもどんどん使っていただくんだと思うんですけども、学生さんをどんどん育てていただければなと思います。

佐々木：

ビジネススクールだけではなくて、他の学部にもぜひ寄付講座をいただければありがたいと思います。（笑）

それでは、前園さんはいかがでしょうか。

前園：

講演の中で駆け足で言ってしまったんですけども、スタンフォード大学と一緒にｄスクールという講座にも、われわれSAPも関与させて頂いていますし、例えば、スタンフォードの優秀な学生さんたちがスタートアップする際に、そのアイデアに対してわれわれのクラウド環境を無償で貸し出してモックアップをどんどん作って試してもらう場なども提供しています。パロアルト以外では、ポツダム大学とも新しいものを一緒につくろうということで、大学と実は近しいところでイノベーション事業を展開させていただいています。

最近では、日本の大企業の経営者の方、中には政府、金融機関、銀行の方ですとか、製造業も含めて、トップから管理職の方まで、多くの日本人の方がわれわれのパロアルトのイノベーションセンターにお越しいただいています。

これを、今後はどういうふうにできるかというところもあるのですが、例えば、われわれはそういうアセットを持っていますので、例えば、早稲田の学生さんがそういう何かツアーを組まれて見学に行っていただくというのも一つでしょうし、あとは日本の大学の中にわれわれがイノベーションセンターを一緒に展開するというのは、われわれのほうからはまだ手を挙げていませんけども、例えば、佐々木先生のところとか早稲田の方が、日本で先陣を切ってやろうということであれば、そういうところでのご支援というのは一つありなのかなと思いますし、ぜひそういう世界も見ていただきたいなと思います。

佐々木：

実は、実は私が所属する会計研究科は、SAP さんとは、前から寄付講座等をいただくなどの関係がございまして、それで昨年 11 月に産業経営研究所の高瀬所長などと一緒にパロ・アルトの SAP のラボと、それからスタンフォードのｄスクールを見学させていただきまして、非常に衝撃を受けました。「ああ、こういうところで若くて元気の良い連中がイノベーションを必死になってやっているんだな」と感じました。早稲田でもこういうものをつくりたいね、という話を実は今いろいろな人にしています。

特に、われわれの学校というのは、どちらかというと、そういう勢いのある、勉強よりもそちらのほうが好きだというような学生が結構いると思いますので、ぜひ今後もそういうことのご協力等々をいただければありがたいと思います。インターンシップなどもあるようですから、あのラボには、ぜひ学生に行って貰いたいですね。

前園：

そういうのも当然あるでしょうし。あと、最近、アメリカの大学を出た日本の学生さんが、そのまま、あのパロアルトのイノベーションセンターに就職をされるという例も増えています。

佐々木：

では、宝木さん、いかがでしょうか。

宝木：

若い研究者、特に研究人材というのは、非常に意義があるというか、われわれの研究の将来の後継者として期待しているところです。そういう観点で、産総研としては幾つかそういう人材交流、育成のプログラムがありまして、より具体的に言うと、例えば、佐々木先生のところの学生さんが論文を書いていると。他社のブロックチェーンとかゼロ知識証明の部分で、少し産総研といろいろ交流したいというニーズがありましたら、リサーチアシスタントという制度があります。それは、産総研の研究者と一緒に論文を書くとか研究をするという制度がありまして、具体的には、例えば、

修士課程の方ですと、平均して月７日来た場合は、月額８万円お支払いすると。そのかわり、産総研の研究者のお手伝いという位置付けでお出しします。ただし､その研究者が学会発表する場合は、それは産総研の費用でもちろん行ってもらうということです。博士課程の場合はもうちょっと高くなりまして、月 14 日平均で来られた場合は、月 20 万出ます。これは平均ですので、例えば、夏休みにまとめて来ていただいてもいいですし、１年に引き延ばしてもいいのですけれど。これが一番お薦めです。

それ以外に、連携大学院の制度とか、研究者間のクロスアポイントの制度というのもあります。クロスアポイントは、早稲田の別の学科とはすでに産総研はやっております。この場合、どちらかというと教授クラスの人材交換なので、より本格的な研究になるかと思うのですけれども。いろいろそろっておりますので、ご興味のある方は、産総研のホームページを、今言ったリサーチアシスタントとか、見ていただければ、より具体的に検討できるかと思います。以上です。

佐々木：

今度は学内の立場から。久保田先生にお願いいたします。

久保田：

法学部では、国際取引法の中で１時間ぐらい、ロースクールでは電子商取引法で１時間程度しか扱っていないので今後改善の余地があります。その他、この会場におられた方に多少お役に立てる可能性があるのは、国際取引法学会という学会で、今年からエッセイコンテストというのを始めまして、学部生の部と院生、社会人の部があります。最優秀賞は、お金や賞がもらえて、賞がもらえれば、早稲田生だったら早稲田の学生文化賞につながるというメリットがあり、賞も多数出しております。９割方商学の分析であって、１割だけ法律が書いてあるのでも OK ですので、われと思う方はぜひ国際取引法学会のホームページを見て応募していただければ幸いです。以上です。

佐々木：

ありがとうございます。

長丁場でしたが、私にとってとてもうれしいのは、このパネルディスカッションまで、若い人が非常にたくさん会場に残ってくれているということです。今日は、これから新しい時代にどうチャレンジしていったらいいのか、という示唆も皆さんからたくさんいただけたと思います。ぜひ早稲田だけではなくて、日本全体がもうちょっと元気になるような、そういうことができたらいいなというふうに思っております。

ということで、ちょうど時間がまいりましたので、今日はこれくらいで失礼いたします。どうも皆さん、ありがとございました。

司会：

パネリストの皆様､大変ありがとうございました。今一度盛大な拍手をいただければと思います。

それでは、これをもちまして第 25 回産研アカデミックフォーラムを終了いたします。お帰りの際には、アンケート用紙を入り口で回収しておりますので、ご協力のほどよろしくお願い申し上げます。本日は、ご来場いただきまして誠にありがとうございました。

第25回　産研アカデミックフォーラム

ブロックチェーンが切り拓く未来

2017年5月13日（土）
12:30 ～ 18:00

大隈記念講堂小講堂
〔収容 300 名〕

プログラム（敬称略）

12：30～12：35　開会挨拶

■イントロダクション：ブロックチェーンとは何か？
12：35～13：00 「石貨・仮想通貨・ブロックチェーン」
早稲田大学商学学術院教授　佐々木 宏夫

■第一部：ブロックチェーンの活用
13：00～13：40
【講演1】「銀行におけるブロックチェーン技術の活用可能性と課題」
三井住友銀行　ITイノベーション推進部　竹田　達哉

13：40～14：20
【講演2】「SAPが支援したブロックチェーン適用ケースと、そこから学んだこと」
SAPジャパン　ソリューション統括本部　岡田　和也

14：20～15：00
【講演3】「個人情報の有効活用を可能にするブロックチェーンの考察」
産業技術総合研究所 情報技術研究部門　宝木　和夫

■第二部：ブロックチェーンの法的・経済学的論点
15：00～15：40
【講演4】「ブロックチェーンの法的課題」
早稲田大学法務研究科教授　久保田　隆

15：40～16：20
【講演5】「ブロックチェーンは経済社会をどう変えるか」
早稲田大学商学学術院教授　佐々木 宏夫

■第三部：パネルディスカッション
16：30～18：00 「ブロックチェーンの可能性と限界」
パネリスト：竹田 達哉／宝木 和夫／久保田 隆／
前園 曙宏（SAPジャパン シニアディレクター）
司　　会：佐々木宏夫

定員：300名　聴講をご希望の方は、早稲田大学産業経営研究所ホームページより専用フォームにてお申し込みください。申し込み締め切り：2017年5月10日（水）。締切日以降は当日申込みとなります。ただし、定員になり次第締め切る場合があります。

対象：学生、教職員、一般どなたでも聴講頂けます。聴講無料。

早稲田大学産業経営研究所　〒169-8050東京都新宿区西早稲田1-6-1 早稲田大学11号館3階
TEL：03-3203-9857　E-mail：riba@list.waseda.jp　担当：小林・荒瀬
ホームページ：http://www.waseda.jp/sanken/

産業経営研究所スタッフ

高瀬　浩一（所　　長）　早稲田大学　商学学術院教授
八重倉　孝（所長補佐）　早稲田大学　商学学術院教授
根岸　亮平（助　　手）　早稲田大学大学院商学研究科　博士後期課程
佐々木博之（助　　手）　早稲田大学大学院商学研究科　博士後期課程
井口　　衡（助　　手）　早稲田大学大学院商学研究科　博士後期課程

産研アカデミック・フォーラム No. 25

2017年２月20日発行

発行者　　早稲田大学産業経営研究所所長　高瀬　浩一
発行所　　早稲田大学産業経営研究所
〒169-8050　東京都新宿区西早稲田１－６－１
電話（03）3203-9857
FAX（03）3202-4274
印刷所　　照栄印刷株式会社