近未来金融システム創造プログラム第 １３回講義レポート

第１３回講義は、早稲田大学大学院経営管理研究科の斉藤賢爾先生から「ブロックチェーンと金融システム」という題で講義があった。本年度は、近未来金融システム創造プログラムの４期生が指定討論者・指定質問者としてオンライン講義に参加しており、Zoomのチャット機能を使った活発な議論も行われている。

電気係は、もう要らない

アメリカの人類学者のデヴィッド・グレーバーの「ブルシット・ジョブ」によると、今の時代には多くの仕事がブルシット・ジョブ（無意味であったり、機械による代替や自動化などが出来る業務）である。最近でも、小学校のある教室に先生が「電気つけて」と言うと電気をつける係がいたという。小学校という場所が子どもが社会に出るための訓練を受けている場所だとすると、電気係りという役割はその本質をえぐり出している（ブルシット・ジョブをこなすための訓練を受けている）ことが分かる。本来なら、現代における我々は、電気係ではなく「Alexa、電気つけて」と一言いえば機械がその役割を担ってくれるはずである。

人類が資本主義の中で構築してきたシステムは、20世紀後半までにはブルジョワジー（資本家階級）が「電気つけて」と言うと、プロレタリアート（労働者階級）が「はい」と答えるような仕組みになっていたとも言える。この仕組が21世紀に入ってからはAlexaなどの人工知能が「はい」と答える自動システム側の仕組みに除々に移行している。この現象が極端に進むと、技術社会環境が自然環境と等しくなる「超自動化分散社会環境」が出現するのではないかという議論もある。今までは、鉛筆１本の製造を行うにも大勢の手がかかる分業システムにより実現してきたが、自動化された工場などで木材などの木料が自ずと鉛筆になる仕組みを構築できると、人間にとって、鉛筆は木になる自然なものとして自然環境が技術によって拡張されるようになる。今後は、20世紀にかけて作り上げてきた分業システムから自動システムに移行する流れが進むと考えられる。

ブロックチェーンの特徴とその作り方

ブロックチェーンに関しては未だに誤解や誤った報道が多い。メディアなどでブロックチェーンを暗号化という文脈で取り上げることがあるが、これは間違いである。暗号化とは、情報を符号化するプロセスで、平文を暗号文に変換することを意味する。また、許可された者のみが、暗号文を復号して平文に戻し、元の情報にアクセスすることが出来る仕組みである。この前提で考えれば、ブロックチェーンを設計し稼働させる際には、ブロックチェーン本体には暗号化は要らない。暗号化を用いるのはクライアントが秘密鍵を使用する時であり、ブロックチェーンやビットコインの動作と直接的な関係はない。

ブロックチェーンは、元々ビットコインを生み出すために発明されたものである。ビットコインは、自分が持つ貨幣資産を誰かに送ることを誰にも止めさせないという目標を達成するために考案されたものだが、３つのブロックチェーンの特徴がこれを成り立たさせている。第一に（BP1）、

可能な状態遷移を起こせるのは権限を勝手に発揮できる本人のみであるということだ。既存の銀行システムでは、銀行が管理者として暗証番号の入力などを要請するが、ブロックチェーン技術は自分が主体となり権限を発揮できる。第二に（BP２）、本人が望むならそのような状態遷移は必ず起こすことができる。第三には（BP３）、一度起きた状態遷移は過去の記録として事実上覆せない。この３つの条件が揃うと貨幣資産を誰かに送ることを誰にも止めさせない仕組みが構築できる。

この３つの特徴を実現するための基本的な考え方として、状態マシンの複製がある。状態マシンの複製という概念は、1984年に耐障害性を維持する目的でランポートがまとめたものだった。ブロックチェーンでも状態マシンの複製と同様にジェネシスブロックという（１）等しい初期状態から始まり、（２）全ての参加ノードにイベントがコピーされる。ここでのイベントはトランザクションとそれが集まったブロックを意味し、これらは（３）同じ順序でコピーされる。また、（４）全イベントは状態に対してどのノードでも等しく作用する（非決定的でなく決定的である）という４つの要素を満たすので、耐障害性を満たす。

ブロックチェーンは、状態マシンの複製に加えて、全体を自発的に参加できる自律分散的な競争プロセスを置くという考え方がある。状態マシンによって誰もがレプリカをもち、正しい記録かどうか検証できる仕組みを構築し、更に多くの目で見張れるという新聞モデルを導入することによってBP３を満たすという考え方である。この競争プロセスが特定の権力者を置かずに止まらないというルールのもとで行われるとBP１とBP２も満たせる。

ビットコインなどのブロックチェーンの改ざんが難しい理由は、ブロックのダイジェストを典型的には手前のブロックから引き継いでいるターゲット以下の値にしなければならないからである。現在では、（ビットコインでは平均１０分の間に）ターゲット以下のダイジェストが出てくるまで、一秒当たりエクサハッシュ（垓）の計算を繰り返す必要がある。もし、改ざんを加えたいのであれば、このエクサハッシュという計算を行わなければならないが、コストの問題から事実上不可能（あえて挑戦する者がいない）という仕組みになっている。ブロックを作るためには、そのダイジェストがある数以下という条件を満たす（Proof of Work）か、仮想通貨の持ち分に応じた権利を使った投票で勝つ（Proof of Stake）必要がある。ナカモトコンセンサスは、このように最もコストが掛かった歴史（一番改ざんが難しい歴史）に全員が一致するという仕組みである。

Proof of Worksのコストは、端的にいうと電気代である。マイナー達は、最近のターゲットを基に、そのコストを掛けた結果どれくらいの収益を得られるのかという期待値を計算できる。つまり、その期待値によってマイナー達が掛けられる電気代は自ずと決まって来る。期待値はその仮想通貨の市場価値によって決まるので、その変動に応じてマイナーの参入と撤退が決まり、長期的には市場価値とコストが均衡する仕組みになっている。Proof of Worksで改ざんが難しくなっているのは、その仮想通貨の市場価値が高く維持されているからだ。現在のブロックチェーンは、

コストを掛ければ改ざんが不可能ではないという意味で、攻撃が成功すると全員の新聞が切り替わる「買収可能な新聞モデル」に留まっている。

ブロックチェーンの存在意義は、デジタル署名と深い関わりがある。人々がデジタルの世界で何かを証明する（現状知られている）唯一の手段であるデジタル署名の実用化の課題として、経時証明問題とアリバイ証明問題が挙げられる。過去に施された署名を正しいと証明できることをデジタル署名の「経時証明問題」と言い、過去に施されなかった署名が実際に存在しないことや、偽装された過去の署名を正しくないと証明できることを「アリバイ証明問題」と言うが、公開鍵証明書の期限切れや秘密鍵の漏洩の可能性などが存在するため困難である。正しく動作する（BP1-３を満たす）ブロックチェーン技術があれば、署名付きの文書（例えば、遺言書）のダイジェストをブロックチェーンに書き込むことによって、この問題を解決できる。秘密鍵が漏洩してもそれまでの時点の記録は正しいと言えるし、過去に存在しなかったかを全て証明することが不可能だが、少なくともブロックチェーンシステムの中には記録されてないという証明ができる。ブロックチェーン技術は、デジタル世界上での経時証明問題とアリバイ証明問題に対する解決策を示している。

続・電気係は、もう要らない

ブロックチェーンという実証方法によって我々が追求しているのは、記録が正しく保全・アクセスできるようにデジタル拡張されたレッジャー（台帳・帳簿）である。その真価は、過去に位置づけられたデジタル署名を、何の権威にも依らず正しい又は正しくないと証明できるようになることだ。レッジャーの存在は、記録の公正性のレベルを押し上げ、支払い・会計・登記・契約から行政・立法・司法をも含む社会基盤を遥かに軽やかにする変化を巻き起こす可能性を秘めている。

より具体的な例で言うと、公証役場や法務局、監査機関のようなものを自分で立てられるようになる。第３者の保証なしに当事者間の契約を証明できるため、従来の公証サービスを使う行為が（現状ですら面倒だが）著しく面倒くさくなる。また、その非中央集権的な特徴によって、銀行ネットワークをバイパスする送金システムも構築できるため、銀行・金融機関の解体が進む。それに加えて、自由に貨幣媒体の仕組みを設計できるようにもなる。

Q&A

続く質疑応答においては、以下のような点が主に論じられた。

Q.以前、記事などでブロックチェーンによって与信ができると聞きましたが、これは個人を安易に裁くことに繋がり、怖いなと思いました。ブロックチェーンを活用して行くには、そういった面もハードルがあると思いますが、その点について教えて頂けますと幸いです。

A.プライバシーに関わることはブロックチェーンで実現することではないです。ただ、情報をも

らった側が正しい情報をもらっているかの検証がブロックチェーンによって可能です。個人はアプリとサービスのレベルで、誰にどういう情報を出すのかをしっかり決めて行くのが大事ですが、これはブロックチェーンとはまた別の問題です。偽の情報が流れないようにすることは（BP1-3が満たされている限りにおいて）ブロックチェーンで可能です。

Q. ブロックチェーンを使って、記録をパブリックに晒すことのメリットを生かした応用として仮想通貨以外に何かあるでしょうか？　（クローズにしていて、真贋が問題になった時だけ晒せば良いような気がします。）

A.基本、真贋の問題になったときは晒せば良いと思います。データが出来てきた時にそれが本物かどうかを見れば良いです。よくブロックチェーンを応用しているという人で、「ブロックチェーンに暗号化したデータを入れています」と言う人と会うのですが、暗号化というのは鍵を持っていると復号できるので、危なっかしいと思います。ダイジェストが破られることもあると思いますけど、鍵が漏洩するなどのレベルではない水準で守ることができるわけです。