近未来金融システム創造プログラム講義レポート

第十三回となる本講義では、早稲田大学大学院経営管理研究科教授の斉藤賢爾様から、「金融と技術（各論Ⅴ）ブロックチェーンと金融システム」という題目で、暗号資産とブロックチェーンの成り立ちから、暗号資産を巡る経済の仕組みについて講義が行われた。

暗号資産の成り立ちとその経済学

暗号資産とは、不特定の者に対して支払い等に使用でき、法定通貨と相互に交換できるが法定通貨建てではない電子的媒体のことである。ブロックチェーンにより実現されるものであるが、社会全体にとってはその重要性は必ずしも大きいとは限らない。

ブロックチェーンの設計におけるゴールとして、以下の 4 つの性質が挙げられる。

1. 自己主権性: ユーザーの意思だけで参加し送金指示できる
2. 耐検閲性: 送金記録やその確認は他者の意思では妨げられない
3. 耐障害性: 送金の記録やその確認はシステムの故障によっても妨げられない
4. 耐改ざん性: 送金の記録を抹消・改変・捏造できない

この 4 つの性質が揃うことで、いかなる方法によっても(送金)記録の否定ができないようになる。また、暗号資産は暗号化されているという誤解があるが、ブロックチェーン自体は暗号化されていない。ただ、ウォレットで秘密鍵が暗号化されるなど、一部で暗号技術が使用されている。加えて、ブロックチェーンは厳密な匿名性を目指したものではなく、自由で妨害されない取引を可能にすることが主な目的である。さらに、ブロックチェーン特有の技術としての動作条件は、ネイティブ暗号資産の市場価格が十分に高いことである。この価格依存性は、技術として異例の動作条件であり、価格が下がればブロックチェーンが適切に機能しなくなる可能性がある。このように、ブロックチェーンには動作条件や特有の制約があるが、その設計思想には「検閲されない自由な取引」を実現する意図が強く反映されている。

では、ブロックチェーンとはそもそも何なのか。ブロックチェーンは、コストレジスター付きの分散型台帳システムであり、大勢の独立した参加者が協力して台帳を維持する仕組みである。新しいブロックを追加する際には、これまでの履歴に蓄積されたコストを増大させるようなものでないのならば変更は生じることはなく、そのコストはネイティブ暗号資産建てで測られる。ブロックチェーンの自己主権性は、公開鍵暗号を活用した仕組みによって担保されており、誰でも自由にアカウントを生成し、取引に参加できる。さらに、耐検閲性と耐障害性は、大勢の独立したコンピューターが冗長性を持って運用されることで、特定の取引が止められたり、システム障害によって記録が妨げられたりしないよう確保されている。耐改ざん性については、改ざんを試みる側がコスト負担ベースでマイノリティーである場合に成立する仕組みとなっている。これらの性質を支える技術的要件として、分散システムの冗長性や P2P ネットワークが挙げられるが、同時に、参加者が台帳維持に参加する動機も

重要である。具体的には、参加者はネイティブ暗号資産という報酬を得ることを目的としてコストを負担し、その結果としてブロックチェーンの正当性が保たれている。このように、ブロックチェーンは技術的要件と動機的要因が融合した仕組みによって、分散型台帳の信頼性と安定性を実現している。ここで、動機的要因の話をする前に基礎的な技術である、暗号学的ハッシュ関数とデジタル署名について紹介する。

暗号学的ハッシュ関数とは、任意のデジタルデータを入力として受け取り、固定長の出力（ハッシュ値）を生成する関数であり、その特徴は一方向性と一様な分布性にある。一方向性とは、生成されたハッシュ値から元のデータを逆算できない性質を指し、これにより暗号学的な安全性が確保される。また、一様な分布性とは、入力データがどのように偏っていても、出力されるハッシュ値が全空間に均等に分布する性質であり、衝突（異なる入力が同じハッシュ値を生成すること）が極めて起こりにくい設計となっている。暗号学的ハッシュ関数には SHA-2 や SHA-3 といった標準化されたアルゴリズムがあり、それらは例えば 256 ビット長のハッシュ値を生成する。これらの関数は、法則性が見えないマッピングを行い、逆方向の計算を事実上不可能にする性質を持つ。唯一の方法はブルートフォースで 1 つずつ試行する方法であるが、現実的には非効率的である。衝突が発見されると暗号学的安全性が失われ、そのハッシュ関数は使用できなくなる。実際、SHA-1 は衝突が発見されたため、現在では非推奨とされており、将来的に使用が完全に廃止される予定である。これらの性質により、暗号学的ハッシュ関数はブロックチェーンのブロックヘッダ等の多くの場所に利用されている。

デジタル署名は暗号化とは異なり、復号を伴わないため暗号化の範疇には入らないが、データの整合性と署名者の意思確認を担保する仕組みである。ビットコインやイーサリアムでは、署名者が秘密鍵を用いて取引データ（トランザクション）に署名を施し、その署名、元のデータ、公開鍵をセットにしてネットワーク上に送信する。この情報はブロックチェーンに記録され、検証者（マイナーやバリデーター）によって正当性が確認される。検証では、公開鍵と署名、元のデータを用いて、署名が本当に対応する秘密鍵から生成されたものであるか、また元のデータが改ざんされていないかを確認する。また、公開鍵のハッシュ値が送信元アドレスと一致することで、取引がそのアドレスの所有者によるものであることが保証される。この仕組みにより、ビットコインやイーサリアムでは送金の正当性とデータの改ざん防止が実現されている。

ブロックチェーンにおいて、各ブロックは取引データを含み、暗号学的ハッシュ関数によるハッシュ値（ダイジェスト）が次のブロックに組み込まれることで連鎖を形成する。この構造により、1 つの取引を改ざんするとその後の全てのブロックのハッシュ値を再計算する必要がある。しかし、この仕組みだけでは安価なマイクロコンピューターですら容易に改ざんが可能であるため、追加の対策が取られている。追加の改ざん対策として、ビットコインでは Proof of Work（作業証明）という方式を採用しており、ブロックのハッシュ値が合意されたターゲット値以下である必要がある。このターゲット値はハッシュ値全体の空間から

見て相対的に非常に小さいため、適切なハッシュ値を見つけるには膨大な計算が必要となり、結果的に改ざんを試みる者がビットコインネットワーク全体の計算能力を超えることが事実上不可能になる。平均して 10 分に 1 回新しいブロックが生成されるペースを追い越して改ざんを行うためには、ネットワーク全体を上回る計算力が必要であり、これが Proof of Work のセキュリティの本質である。一方、イーサリアムは現在 Proof of Stake（掛金証明）を採用しており、参加者は暗号資産をデポジットとして預け入れることでブロック生成に関与する権利を得る。この方式では、デポジット量に応じた投票権が与えられ、2/3 以上の投票を得たブロックが最終的に確定する。悪意ある行為者がネットワークの動作を妨害するには全体の 1/3 以上の資産を買い占める必要があるが、それが現実的に困難である点で安全性が担保される。ただし、イーサリアムの市場価格が大幅に下落した場合には、このコストが低下し安全性に影響を与える可能性がある。ビットコインの Proof of Work（作業証明）についてもう少し詳しく説明する。Proof of Work は参加者がくじ引きのように繰り返しダイジェストを計算する仕組みであり、この計算には電力コストがかかる。平均して 10 分間に 1 回誰かがくじ引きに当たるように設計されており、当選確率は投入した電力コストに比例する。参加者は、ビットコインの市場価格が電力コストを上回る場合に利益を得られるため、この仕組みをビジネスとして捉える。利益が見込めると新規参入者が増え、計算力が上昇し、ブロック生成時間が短縮される。その際、ネットワークはターゲット値を引き下げて計算を難化させ、再び平均 10 分間に 1 回のペースを維持する。一方で、電力コストが市場価格を上回ると採算が取れなくなるため、参加者は撤退し、ハッシュパワーが低下する。この場合、ターゲット値が引き上げられ、計算が容易になることで必要な電力コストが減少し、均衡が保たれる。このプロセスを通じて、電力コストとビットコインの市場価格は動的にバランスし、Proof of Work の仕組み全体が安定的に機能するよう設計されている。

ビットコインのネットワークでは、全体の計算能力を示すハッシュレートが現在ピークで約 780 エクサハッシュ/秒に達しており、これは電力コストの増大と密接に関連している。この計算能力を支えるエネルギー消費量は推定で約 17GW に相当し、これは大阪市や横浜市の総エネルギー消費量に匹敵する規模である。前述のように、ビットコインの価格が上昇すると利益を求めて参入者が増え、ハッシュレートも増加する一方、価格が下がると撤退が起きてハッシュレートが減少するという動的な調整が行われる。この 17GW というエネルギー消費量を、太陽光発電のキャパシティと比較すると、現在の地球規模の太陽光発電能力はさらに大きく、このエネルギーを特定の目的に集中して使用することも理論的には可能である。例えば、世界には太陽光発電のみでビットコインネットワークを攻撃可能な計算力を持つ国が 13 カ国存在する。このような比較は、ビットコインのエネルギー消費が巨大である一方で、再生可能エネルギーの拡大がその影響を相対化しつつあることを示している。

最初から伝統的金融に呑まれていた分散型金融

暗号資産取引市場やDAO（分散型自律組織）は、ネイティブ暗号資産の市場価格に依存して成り立っている。暗号資産取引の多くはブロックチェーン上で実際に移転するわけではなく、取引所の台帳に記録される所有残高を基に取引されている。この構造により、ETFのように抽象化されているが、基盤となる暗号資産の価格変動に大きく左右される点で脆弱性が高い。

DAOの本来の概念は、自律的に動作するシステムが人間を雇い、特定のタスクを遂行することであったが、現在ではスマートコントラクトを用いて経営ルールを記述し、トークンを発行して投票権を割り当て、意思決定を行う形式が主流となっている。しかし、多くのDAOが明確な目的を欠き、トークンの値上がりを狙う参加者に支配されがちで、株式会社や合同会社の模倣にとどまるケースも多い。結局のところ、これらの組織も暗号資産の市場価格に頼っており、価格が急変すれば成り立たなくなる可能性がある。

上でも述べたが、ブロックチェーンは、送金記録の否定を防ぐ仕組みを持ち、ネイティブ暗号資産による経済的インセンティブと高いコストによる防御性を通じて、冗長性とセキュリティを確保している。しかし、その動作条件はネイティブ暗号資産の市場価格が十分に高いことに依存しており、価格が需要によって決定される構造のため、伝統的産業との直接的な接点が希薄である。しかし、ビットコインのマイニングでは太陽光発電のようなコストの低い再生可能エネルギーの活用が進むと予想され、再生エネルギーへの投資を呼び込む可能性がある。一方で、イーサリアムのProof of Stakeには社会的価値や産業的接点の明確な意義が見出しにくい。その需要は手持ち資産の価値を上げることを目的としたプロモーションや、地下経済における追跡困難な送金手段としての利用に支えられている。この仕組みは先行者に利益をもたらす構造であり、伝統的金融の投資家からも一時的な注目を集める一方、産業基盤がないため、ポンジスキームと類似していると考えている。先行者利益は後続の投資家による資金に依存しており、ネイティブ暗号資産が暴落すれば、このシステム全体が停止するリスクが高い。以上の点から、暗号資産やブロックチェーンの現状は、多くの課題を抱えた状態であり、社会的価値や実質的な産業基盤の不足が指摘される一方で、投機的要素によって維持されている脆弱なエコシステムであると考えている。

最後に

これからの社会では、自動化と技術進化の影響により、分業社会の終焉と狩猟採集社会に近い新しい形態への移行が進む可能性がある。従来の分業社会では、BULL SHIT JOBと呼ばれる、不必要だが高待遇の仕事が蔓延し、一方で必要でありながら低待遇のSHIT JOBが存在してきた。しかし、自動化が進むことで、これらの役割の多くが不要となり、人間はAIや自動システムとの「調整」を通じて新たな生活を営むようになる。

この状況は、技術の進化を分析する「テトラッド」の視点から見ると、社会が特定の技術によって強化される一方で、過去に押し込められた要素が復活するという構造の再現だと言

える。例えば、自動運転車が登場すると、馬による移動の制約(すなわち、人間と人間以外の知性が協力して移動する)と同パターンの新たな制約が生じるように、古い要素が新しい形で蘇る。このように、技術の進化は新たな問題を生むが、それを解決する技術の登場によって社会構造が循環的に変化していく。

さらに、狩猟採集社会が持っていた協働やコラボレーションの要素が再び重要になり、支配構造を伴わない社会の在り方が見直される可能性がある。この文脈で、貨幣や金融経済の意味が問われることになる。貨幣が引き続き必要とされるのか、あるいは新たな経済システムに置き換わるのかについては、今後の社会的変化による検討が求められる。こうした問いが、これからの技術社会における人間の役割と共に議論されていくべきである。

Q&A

Q. 斉藤様は Bitcoin に対してどのようなポジションなのか。理論からデジタル通貨を考えている人にとって暗号通貨は存在意義のあるものと考えているのか。

A. 一貫して批判を続けている。

Q. 暗号資産の価値は、ネイティブ暗号資産の価値が高い前提だと考えている。量子コンピュータなど、コストベースで高い計算処理ができるようになると、暗号資産の価値はどのようになるのか。

A. 量子アルゴリズムとして脅威になるのは Shor のアルゴリズム(デジタル署名を破りうる）や Grover のアルゴリズム(暗号学的ハッシュ関数を破りうる）等で、それぞれ対策が知られている。それぞれを用いた攻撃が実用的になるまでの時間内で対策を実装しデプロイできれば問題にはならないだろう。Ethereum はおそらく余裕をもってハードフォーク(ブロックチェーンのプロトコルを過去と非互換なものに変更）によりこれらに対応できる。価格には影響無し、ないしポジティブに影響するだろう。Bitcoin は間に合わない可能性があり、価格にネガティブに影響するだろう。これは技術の問題ではなく、技術ガバナンスの問題で、Ethereum の方が技術をガバナンスする主体が明確だからであって、それはある意味で中央を排除するのに失敗しているため、自律分散システムとして見た場合に良し悪しがある。

Q. 日本には仮想通貨に対する規制が進んでいる。アメリカのような規制緩和は必要だと思

うが、日本に必要なアクションは何か。

A. 暗号資産(というか貨幣的価値の追求全般）にいち早く見切りをつけて、より本質的な課題に取り組むことだと思う。より本質的な課題というのは、例えば AGI（人工一般知能）が十分に普及した状況下における新しい経済構造（おそらく貨幣は無意味になる）を考えることである。

Q. 暗号通貨が金融経済に取り込まれず従来の中央集権的な貨幣として成立するためにはどうすればよかったと考えているか。

A. 私は暗号資産がこの世から消えて無くなればよいと思っているので、貨幣として成立して欲しくない。その上で、あえて暗号資産が従来の貨幣のようになるためにはどうすればよいかと言えば、国家が Ethereum PoS と Ether 市場をスーパバイズするようなイメージの暗号資産にすればよいのではないだろうか。ただし、貨幣としての使用は Rollup(セカンドレイヤ)で行わないと実用的にはならないと思う。