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 回目となる本日は、早稲田大学大学院経営管理研究科（早稲田大学ビジネススクール）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これからの金融システム」という題目で講義が行われた。斉藤様からは暗号資産とブロックチェーンの成り立ちや仕組みついてご教示いただいた。また、今回の講義の後半では金融の消滅という未来についてお話をいただいた。

1. 暗号資産とブロックチェーンの基本設計

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である。本講義では、ブロックチェーンにより実現されるものを対象とする。ビットコインは「自分が持つコインを自分だけが自由に誰かに送るのを誰にも止めさせない」という目的のために、ブロックチェーン技術とともに発明された。

ブロックチェーンの設計は、4 つの重要な性質を満たすことを目指している。第一に自己主権性であり、ユーザーの意思のみで参加し送金指示できることを意味する。つまりアカウントを勝手に作れる必要がある。第二に狭義の耐検閲性であり、送金の記録やその確認は他者の意思では妨げられない。第三に耐障害性であり、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。第四に耐改ざん性であり、送金の記録を抹消・改変・捏造できないことである。

これらをひっくるめると広義の耐検閲性と呼ぶことができる。つまり、いかなる方法によっても送金記録の否定ができないということである。この実現のために、これら 4 つの性質が満たされていることをユーザーが確認できなければならず、そのためには記録が公開されていることが原理的に必須となる。したがって、実装する上では暗号化は基本的に使わない。暗号資産と言われているが、実際には暗号化されているわけではない。暗号化が使われるのは、ウォレット側で秘密鍵を守る場合などに限られる。

他のすべての技術がそうであるように、ブロックチェーンには動作条件が存在する。特有の動作条件として重要なのが「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。この条件が満たされないとシステムが正常に動作しない。価格は操作可能であるため、AI によって人々のマインドが誘導され価格が下落すると、ブロックチェーンの維持のために働く参加者が減少し、システムの維持が困難になる可能性がある。

2. ブロックチェーンの技術的仕組みとコスト構造

ブロックチェーンは、「コストレジスター付き台帳」として抽象化できる。新しいブロックを作ってコストをかけて記録し、それが全体に加えられていく。通常は追記されていれ

ばコストが上がるので問題ないが、記録を書き換えようとすると過去に遡るほど大きなコストがかかる。書き換えた時点から現在までのコストをもう一度負担しないと変更できないという仕組みで、書き換えを防いでいる。

この仕組みを支える要素技術として、暗号学的ハッシュ関数、デジタル署名、ハッシュチェーンがある。暗号学的ハッシュ関数は、入力の集合が無限で出力が 256 ビットなど固定長である。一方向には安価に計算できるが、逆方向には計算できない一方向性を持つ。無限を有限にマッピングするため、異なる入力が同じ出力になる衝突が稀に起きるが、衝突させる方法が見つかった関数は安全とは見なされない。SHA-1 は衝突が見つかったため使わないように徐々に移行しており、現在は SHA-2 シリーズや SHA-3 シリーズが使われている。

デジタル署名は、公開鍵と秘密鍵のペアを用いる。署名者は秘密鍵でデータに対する署名を作り、検証者は公開鍵と元のデータと署名を用いて検証する。典型的なブロックチェーンでは、公開鍵に暗号学的ハッシュ関数をかけてアドレスを生成する。トランザクションに公開鍵と署名が付いているため、そのアドレスを持つ本人であることが確認できる。

ハッシュチェーンでは、ブロック内に取引データが入っており、次のブロックには前のブロックのダイジェストが格納されている。このダイジェストはそのブロックを一意に示す識別子としても用いられる。例えば取引データを削除するとブロックのダイジェストが変わり、次のブロックとの間に矛盾が生じる。ハッシュチェーンの構造だけでは、ブロックを書き換えることに大きなコストは必要ないため、繋がっているブロックのダイジェストを次々と書き換えていけば矛盾なく改ざんできる。極端な例として、1 ブロックの書き換えに 100 万分の 1 秒かかるとして、それを 100 万ブロック分やらないと全体の書き換えが完了しないとしても、1 秒で改ざんが完了することになる。従って、ハッシュチェーンの構造自体がブロックを改ざんから守っているのでは無い。ではどうやって守っているのか。

作業証明（Proof of Work）では、ブロックのダイジェストは、合意されたターゲット値以下でなければならない。暗号学的ハッシュ関数の性質上、どうすればターゲット値以下のダイジェストが得られるかは分からず、ブロックの内容を少しずつ変えながら（そのために NONCE、つまり Number used ONCE と呼ばれる領域がある）、何回も何回も計算する必要がある。

この話をしている現在、ビットコインのピークは 1.1ZH/s（11 垓ハッシュパーセカンド）で、全体で平均すると 600 秒（10 分）に 1 回のペースで誰かが上の条件を満たし、ブロックが生成される。書き換えしようとする場合、新しくブロックを作るペース以上のペースで過去のブロックを書き換えていかないといけない。つまり全体の計算パワーを上回るパワーで書き換えをやっていかないといけないのである。

3. 経済的インセンティブと報酬システム

ユーザーは取引手数料を負担するだけだが、台帳を維持する大きなコストを払って統一した記録を書き込む参加者が存在する。その理由は、確率的に大きな報酬をネイティブ暗号資産で得られるからである。報酬を得るためにはマジョリティ側にいなければならないので、一つの履歴にまとまっていこうという圧力がかかる。

作業証明のコストについて詳しく見ると、参加者はくじ引きのコストを電力で払っている。報酬の期待値が電力コストより大きければ儲かるので参入が起き、くじ引きのパワーが上がる。するとブロック間隔を一定に保つためにターゲット値が引き下げられ、電力コストが上がる。逆に報酬の期待値が電力コストより小さければ損をするので退出が起き、ターゲット値が引き上げられて電力コストが下がる。長期的に見ると、電力コストとネイティブ暗号資産の市場価格の水準は均衡する。

現状のビットコインは、高効率なマイニング ASIC の効率の平均値で計算すると約 24GW の電力を消費している。これは横浜市の総エネルギー消費を超えており、太陽光発電のキャパシティで比較するとオランダ（世界 11 位）に相当する。単独で太陽光発電だけでビットコインに対抗できる国が 11 カ国ある。日本、インド、ヨーロッパなどが突出しており、これらが頑張れば理論的には対抗可能である。

掛け金証明（Proof of Stake）は、コストのかけ方が異なる。イーサリアムでは 32 イーサ（このまとめの当時約 350 万円）以上のデポジットで初めて参加でき、正当なブロックがどれであるかは、デポジット額に応じた投票で決まる。掛け金に比例するブロック報酬をもらうため、メンテナンスコストとイーサリアムの価格のバランスが重要になる。

DAO（分散型自律組織）は、インターネット上に自律的に存在するが、自動システム自身にはできない特定のタスクを担うために人間を雇うことに大きく依存する組織である。内部に資本（報酬として使われ人間を駆動する）を持ち、意思決定を自律的に行う。この内部資本がネイティブ暗号資産であり、その市場価格が十分に高いことで参加者が惹きつけられ、システムが強く防御される。

4. AGI と分業社会の崩壊

金融の未来とは金融の消滅であると考えている。まず AGI（人工一般知能）が実働する世界では、人間のあらゆる肉体労働も知識労働も代替可能になる。人間が現に GI を持っているのだから、AGI の実現は、タイムトラベルのように物理的に困難であったり、永久機関のように不可能なことではない。本当に時間の問題である。これができたとすると、分業社会の意味が損なわれる。

分業社会の脆弱性を見つめる思考実験として、月面で人々が持続的に生きるための社会を考える。ありがちな過ちは地球の経済社会を移植することである。電力や酸素や水や食料といった生存に必須となる資源の生産施設を別々の箇所に設置し、交通網で結び、労働者を置いて賃金を払い、労働者はその賃金で施設から必要な資源を購入する。しかしこの場合、どれかの施設が破壊されると全員が生きていけなくなる。

できるだけ全滅しないためのデザインは、小規模なコミュニティーを数多く地理的に分散させ、それぞれのコミュニティーで独立して電力や酸素や水や食料を生産することである。各人は専門性を身につけるよりも万能であるべきで、AI によるアシストを受けながら、人が人を使役しない世界を作る。この場合、貨幣の出番は無くなる。

地球でも、気候変動、巨大地震、感染症は分業社会の脆弱性を突く攻撃と見なせる。気候変動は台風や洪水を引き起こし、巨大な流通経路を寸断する。感染症に対策する場合はロックダウンが必要だが、そうすると経済が回らなくなる。経済を回すために GoTo 政策のような感染症を蔓延させる政策を取らないと生きていけないという分業社会の脆弱性が露呈する。

技術社会環境は自然環境と同じになっていく。昭和時代には、あたかも小学校の多くの教室にいるという電気係に先生が「電気つけて」と言うような、人が人を使役する社会を完成させたが、令和時代にはアレクサに「電気つけて」と言う。人間にとって技術社会環境は意味的に自然環境と同じような対象へと変化していく。将来出現する超自動化分散社会環境は、拡張された自然環境（メタ・ネイチャー）である。自然から資源を採取し、必要であれば手入れをするように、自動システムに対して手入れをし、システムとの対話の仕方を工夫する。これはプロンプトエンジニアリングという形ですでに現出している、環境との付き合い方のパターンである。

分業社会は人類史的に見ると大規模農業とともに始まった。専門性の分化があり、その役割を果たすことで社会が成立していた。しかし自動システム化すると、専門性が脱落し、分業を前提とした社会構造が崩れる。

5. 貨幣経済の終焉と支配構造の変容

近年の人類学・経済史の研究分野では、貨幣は交換の自然発生的な道具ではなく、むしろ国家が徴税権を通じて人々を管理し、権力構造を維持するために設計した制度装置であるとの見方が強まっている。現代では、国家だけでなくプラットフォーム収奪を担う巨大企業も徴収主体として振る舞い、貨幣による支配構造を形成している。

権力者・支配者が提案するありがちな策がユニバーサル・ベーシックインカム（UBI）である。中央から例外なく全員に対して貨幣を配布し、生活を保障する。一見人道的だが、AGI による自動システム下では新たな奴隷制となる。人々を消費者の地位に固定し、持てる貨幣の分だけ人間が自由であるとするならば、その自由は中央が決めた予算の範囲に制限される。加えて、中央はその自由の配布をいつでも減らしたり止めたりする権限を有している。

貨幣の権力作用には 2 つの方向性がある。第一に「納税の強制」による支配、第二に「支払いと使役」による支配である。市場社会では、消費者が企業を支配できるという関係が生まれ、市場に生きる意味を見出させることで被支配者の不満を緩和していた。しかし UBI 経済では第一の作用だけになり、不安定となる。収奪・テロ・破壊行為・カルト

化・インフラ襲撃の増大の恐れがあり、脱貨幣・脱国家・脱プラットフォームという離脱の動きが起きる。

貨幣があるということは、人が人を使役するということであり、人がお金を払って誰かに自分がやりたくなかったりできなかったりすることを頼んでやってもらうことである。そのための前提として専門性が分化していることが必要である。専門性が分化しない状況では、貨幣の存在意味そのものが失われる。

専門性は自発的なものではない。本来、人類は専門性を持たない方が生存に有利である。自分の食料を生産しないと非常に危険だからである。専門性を分割するには安全保障が必要で、そのために国があった。国が安全保障し、専門性が分化することによって初めて分業ができ、貨幣経済が営まれる。人が人の役に立っているということが生きる意味として重要であり、これをオキュペーション（職業）と呼ぶ。自分の時間が職業によってオキュパイ（占有）されることに意味があった。

自動システム化した時、この意味が消える。専門性が脱落し、分業を前提とした市場での役割という部分が失われる。襲撃やテロなどの不安定性が増大し、ピア・ツー・ピア技術がオープンソース化されることで、人間が権力構造から離脱することが可能になる。
支配者のパラドックスとして、支配の対象が実質的に消失するのに、支配者は何を求めるのかという問題がある。物理的リソースを思いのままに操ることが目的だとしても、それは何のためなのか。独裁から降りない限り、よき人物として記憶されることはない。実際に有効な、より良い方向への変化を起こしていくためには、人類の集合知である AI（AGI）を、人類の集合知をもって使っていく必要がある。人間があまり独善的なことを言わないようにし、協力して使うことで効果が出る。そういうことができない場合、暴力や離脱が起きる。

分業社会（金融貨幣経済）は、交換・消費、貯蓄・投資、専門分化を強化してきたが、極度に強化すると格差が進行し、交換が停滞する。新しい技術であるメタ・ネイチャー（自動化の極限）は、過去に衰退させられていたものを回復させる。つまり、貨幣無き信用システム、贈与経済、専門未分化の狩猟採集社会である。ホモサピエンスが何十万年も続けてきた社会を衰退させることによって分業社会が成立したが、自動化が進むことで再び反転し、かつての社会形態が回復する可能性がある。このパターンこそが、金融の消滅という未来につながるのである。