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 回目の今回は、早稲田大学大学院経営管理研究科の斉藤賢爾教授にご登壇いただいた。斉藤様からは「金融と技術」の 5 回目として「ブロックチェーンと金融システム」という題目で、ブロックチェーンとその役割について語っていただいた。

ブロックチェーンと分散ファイナンス

多くの人が遺言書はデジタル化できると考えているが、遺言書は従来の考え方ではデジタル化できないものの代表例の 1 つである。遺言書に自筆で署名する代わりにデジタル署名を使えば、証人に頼ることなく遺言書が本物だと確認できるのでは、と思われている。デジタル署名は、署名者が秘密に隠し持つ必要のある秘密鍵を使用しているため、署名をする人が秘密鍵を隠し持っているというのがデジタル署名の大前提である。しかし、遺言書は秘密鍵の保持者の死後に使用されるため、秘密鍵にアクセスできる相続人の誰かが不正を働いている可能性があり、改ざんや捏造の危険が伴う。よって、遺言書のデジタル化は従来できなかった。

では、遺言書をデジタル化するためにはどのような条件が要求されるのか。それは、

(1) 遺言書を作成したり更新したりするのが本人だと自分の力だけで証明できる（自己主権性）

(2) 本人が望めば必ず遺言書は作成されたり更新される（耐検閲性、耐障害性）

(3) 遺言書の内容の記録は覆らない（耐改ざん性）

の 3 つの性質が満たされていることを、本人や相続人が検証可能であることが必要とされる。この要求を満たすものとして、ビットコインの送金を可能にするブロックチェーンは設計された。

ビットコインを生み出したサトシ・ナカモトは、「自分が持っているお金をいつでも好きに送金することを誰にも止めさせない」、つまり、「凍結できない資産」を作ることを目的にビットコインを創ったと考えられている。ブロックチェーンは「記録の自由」を目指したテクノロジーであり、そのためには先に説明した自己主権性、耐検閲性、耐障害性、耐改ざん性の 4 つの要素が満たされていることを誰もが検証可能でなければならない。そういうものがあったとして、それを応用するのがスマートコントラクトである。スマートコントラクトは、 4 つの性質がすべて満たされているような台帳にプログラムコードとそれが扱うデータを書き込むという仕組みで、実行のログと状態の変化も書き込んでいくことによって、真正なコードが実行されその結果が正しく共有されていることを全員が確認できるようになっている。

スマートコントラクトの応用の世界

Defi（分散ファイナンス）とは、スマートコントラクトにより実現される金融アプリケーションのことで、より多様な金融取引の形を生み出している。NFT（非代替性トークン）とは、番号で区別されるトークンである。 1 万円札を借りて、別の 1 万円札を返しても問題はないが、NFT はあるものを借りて別のものを代わりに返すことはできない。トークンが番号で区別されているからだ。NFT の所有者は、デジタル署名をしてみせることで、NFT を移転できるため、近代的な所有権を実装しているように見える。しかし、トークン自体に所有の概念を実装できても、トークン ID やメタデータが指すもの（画像など）はスマートコントラクトの管理下に置けなければ処分などはできない （そして一般に管理下には置けない)。

DAO（分散型自律組織）とは、

(1) 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している。

(2) そのため、内部に資本(報酬として使われ人間を駆動する）をもつ。

(3) 意思決定を自律的に行う。

の 3 つを満たすものである。これをスマートコントラクトで実現すると、コントラクトは外部から呼び出す必要があり、自発的には実行されないため、コントラクトを実行するかしないかという意思決定の問題が生じる。そのため、意思決定の自律性という DAO の要素は未完成または脆弱となる。DAO により組織を変化させる手順の中では、コントラクトを呼び出す際に不可避的に特定の人間の判断を通すか、あるいは不特定の人間に執行を委ねるからだ。

Web1.0 は、ハイパーテキストとインターネットを組み合わせて、誰もがデータの生産者になれるポテンシャルを生み出した。最初のユーザは研究者たちであり、もとからデータ（論文）の生産者である人たちであった。そのため、誰もがデータの生産者になれるポテンシャルはあったが、データは研究者や先駆的なユーザのような一部の人間だけが生産できるものだと捉えられていた。続く Web2.0 では、誰もが簡単にデータの生産者になれるようになった。Web3.0 が開発された後、本来の Web の姿からは逸れて、「なんでも金融トークン化しろ」というイデオロギーを持つ、Web1.0 ~ Web3.0 とは似つかない Web3 が生まれた。

貨幣・金融の未来

「電気係は、もういらない。」という話がある。ある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。しかし、その仕事は先生本人がやれば済む

仕事である。社会に出る訓練をする義務教育の場において、この係はなんの訓練になっているのだろうか。このように、本来やる必要のない仕事は、社会にも存在しており、ブルシット・ジョブと呼ばれている。現代は、「電気係」から「Alexa, 電気つけて」になっている。人間を道具として使役する状況から、自動システムを道具として使う状況に変わってきている。つまり、これは本質的には「分業」の終焉の話なのだ。

テトラッドとは、メディア（人と人の間にある人工物すべて）についての 4 つで 1 組の問いかけのことであり、

・強化: それは何を強化し、強調するのか?
・衰退: それは何を廃れさせ、何に取って代わるのか?
・回復: それはかつて廃れてしまった何を回復するのか?
・反転: それは極限まで押し進められたとき何を生みだし、何に転じるのか?

という 4 つの質問から成る。金融貨幣経済システムのテトラッドへの答えとして、金融貨幣経済システムが強化するものは交換・消費、貯蓄・投資、専門分化、農耕・産業社会、衰退させるものは（貨幣無き）信用システム、贈与経済、専門未分化、狩猟採集社会だと考えられる。そして、回復させるものは支配と服従、ヒエラルキー、利益の最大化、反転させるものは格差・未来からの搾取・破産、ブルシット・ジョブ、メタ・ネイチャー(DX の果て)だと考えられる。現在進行しているものが極限まで進むと、かえってそれがかつて衰退させたものと似た仕組みを持つものが登場してくる可能性がある。つまり、デジタルトランスフォーメーションが徹底的に浸透していくと、見かけは違っていても抽象的なレベルでは狩猟採集社会のシステムに似た社会システムが構築されると思われる。しかしこれは、社会が抽象的な意味で似てくるということであり、社会そのものが狩猟採集社会に戻るというわけではない。

この変化は、サイボーグ社会への変化とも考えられる。サイボーグとは、サイバネティックな組織体ということであり、社会がコンピュータという新しい目や耳、手足を持つことである。そこではあらゆることが自動化され、貨幣が不要な社会が訪れる可能性がある。労働の対価としての貨幣というときの「労働」が変化すること、「欲望の二重の一致」がマッチングシステムにより自動化されたり、リソースが公平に生産・配分されたりすることで「交換」自体が不要になることが、その原因である。今当たり前とされている常識は、自動化により当たり前でなくなるだろう。しかし、その新たな目や耳、手足を通して知られた内容が公正であるか、自動化されている仕組みを信頼できるかを考える必要がある。貨幣は、自分で生産できないものを他者から買い取る上で必要となる。逆に見れば、貨幣の存在は専門性の分化によって支えられていると言える。専門性が未分化な社会では、各個人が生きる上で必要な技術は全て自身や小集団で有している。専門性が分化すると、他者に依存しなければ生きられなくなるため、個人の生存確率は低下する。そこで、国による安全保障が必要になる。そのため、貨幣、専門性の分化、国による安全保障は三つ巴の構造にあり、安定してい

た。しかし、DX はこれら 3 つの要素を自動化・効率化・民主化によって破壊する。よって、専門未分化の構造（狩猟採集社会と同じ構造）に社会が変化する可能性がある。

まとめ

「遺言書テスト」には、「持続的耐性」という隠れた問題もある。遺言書は数十年にわたり保守する必要があるが、人類にはデジタル文書を 50 年間保全した経験はまだない。よって、長期にわたって耐える情報インフラを作ることが重要な課題である。これを解決するには、仮想通貨・暗号資産への依存を断ち、新しいブロックチェーンのようなものを設計する必要があると思われる。デジタル技術の進歩とその受容によって消費社会がどう創造的に破壊されるか、何が解くべき問題なのかを考えることが重要である。

Q&A

Q1. ブロックチェーンはどのように発展したのか。

ビットコインが 2000 年代の終わりから起こり始め、10 年代には投資対象になった。ビットコインはソースコードをオープンにしているため、同様のプログラムを持つ仕組みが多くできた。また、そのころにイーサリアムが登場し、イーサリアム上でスマートコントラクトとしてプログラムを動かし、暗号資産を作ることができるため、ブロックチェーンをわざわざ動かす必要がなくなった。また、何らかのプロジェクトを実行する際、そこで使われる暗号資産を先に売りに出すことで資金調達ができるというモデルが誕生した。しかし、これはプロジェクトが継続されないなどの酷い結果につながり、暗号資産も証券のようにきちんと管理されるべきだという意見も出てきた。その間にも、イーサリアムのスマートコントラクト上では大量の DeFi が生まれて、本来の金融の在り方である、どこかの産業に投資が行われて産業が発展するという仕組みとはかけ離れた金融アプリケーションが増加している。

Q2. 交換のマッチングの自動化はどのように行われるのか。

農産物から始まった地産地消という考え方が、近年ではエネルギーの分野にも浸透してきている。このまま、人間が必要とするすべての生産物に地産地消が取り入れられた場合、交換自体が不要になる可能性もあるが、もし交換が必要とされる場合、既存のマッチングアルゴリズムを応用することで交換のマッチングシステムも構築できるだろう。

Q3. 専門未分化な社会に向かっていく指針とは何か。

一番大きなものは、現状を変えていきたいという気持ちである。専門未分化に向かうことは、個人が手元でできる範囲が増えていくことにつながる。専門未分化は、皆が幸福になることを目指した結果として起こるだろうことである。

Q4. 専門未分化により社会が停滞するのではないか。しかし、停滞は成熟とも捉えられるため、悪いことではないのではないか。

人間の能力の限界は確かに成長する上でのボトルネックとなるが、コンピュータは人間を超えたスピードで生産を行えるため、社会が停滞するとは思わない。また、社会の成長が停滞することは、個人が幸福に生きられているのであれば、特に関係しないことである。

Q5. 将来、信用の度合いの評価はどのような形で行われるのでしょうか。デジタルに頼る場合は、NFT 等の形式になるのでしょうか。

デジタルで人間同士の信頼を数値化する必要はないと考える。