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教授の斉藤賢爾様より「金融と技術（各論 V）ブロックチェーンと金融システム」という題目で講義が行われた。

「Web3 におけるリアリティの不在」、「未来における貨幣・金融の不在」という大きく 2 つのテーマについてお話しいただいた。

A 思考/X 思考

2013 年、MIT メディアラボの教授でありパパートの「構築主義」の流れを汲むレズニックは、訪問先である LEGO 社で中国の精華大学の当時の学長、陳吉寧と面会し、陳が考える精華大学の最優先課題が「X 学生」を増やすことだと知る。

「A 学生」は「成績で A を取る」学生で、与えられた課題に取り組み、困難を自分で克服しゴールを達成できる。「X 学生」は、A 学生に比べるとハチャメチャで、既存の体系で評価できない。問題を自ら生み出しリスクを負ってチャレンジする。

2013 年当時、これからの世界に必要なのは X 学生であり X 思考だと言われた。そして、その 10 年後、Open Interpreter は「A 思考は自動化できる」ことを示した。

Web3 におけるリアリティの不在

1989 年に Berners-Lee が Web1.0 を唱え、2005 年に O’ Reilly が Web2.0 を宣言した。そして、遅くとも 2006 年に Berners-Lee は Web3.0 について話した。

Web1.0 は Read、Web2.0 は Read×Write、Web3 は Read×Write×Own と言われることがあるが、これは誤りで、Web1.0 の時代から Read×Write が存在していた。加えて他者へのトラストに依らずにトークンは所有できても、トークンが指したり、包含したりするものは所有できないのであるから Web3 で Own が実現できているとは言えない。

ブロックチェーン編

元々 Bitcoin を可能にするために発明され、「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」ことを目的としていた。銀行のオンライン送金では止められる可能性がある。

ブロックチェーンが満たすべき性質として、ユーザ自身が意思決定して実行できる自己主権性、他者の意思で記録やその確認を妨げられない狭義の耐検閲性、故障によっても記録やその確認を妨げられない耐障害性、過去の記録を抹消・改変・捏造できない耐改ざん性と

いった広義の「耐検閲性」が満たされる必要がある。ブロックチェーンの動作条件は、ネイティブ暗号資産の市場価格が十分に高い状態にあることである。マーケットの売買の状況によって耐検閲性に揺らぎが生じる。これはブロックチェーンの弱点であると言える。それゆえ、公益のために使うことはできない。

ブロックチェーンは参加者によって維持されている。報酬となる ETH の価値は暗号資産の市場価格に依存する。価格が安くなれば参加者は市場から退出する。そして、参加者が少なくなる程、改ざんが容易になる。そのため、ETH の市場価格は高くなければならない。

トランザクションが正当かどうかを確かめるバリデータが動かす Ethereum バーチャルマシンの上でスマートコントラクトが実行される。

スマートコントラクトの実行に必要な計算資源量を Gas と呼ぶ。Ethereum では Gas は ETH でしか買えない。誰かが計算資源量の Gas を買わなければスマートコントラクトは動かない。

現在の Ethereum の仕組みをビーカー/新聞/機械式計算機モデルという物理モデルで説明する。まず、ビーカー、液体、計算機についての前提を述べる。

ビーカーは ETH が入った容器、液体は ETH を指すとする。ビーカーはトランザクション毎に新たに作成するのではなく、秘密鍵とセットで作られ、それぞれ特定の住所に置かれる。秘密鍵で栓を開ければ、中の液体をどこかに注入できる。注がれ口は常に開いていて、液体を注入できる。つまりいつでも ETH を受け取ることができるということである。液体は、機械式計算機が手回しでなく自動で動くための「燃料」として使われる。

計算機は世界に 1 台だけの機械式計算機を使う。広大なメモリを持ち、パンチカードを差し込み、ビーカーをセットすることで動く。プログラマはいきなりパンチカードに打ち込むことはできないため、人間が読めるコードをパンチカードに「コンパイル」するサービスを利用する。

計算機を使う処理を「トランザクション」と呼び、次の 3 種類がある。

(1) 注入元ビーカーと注入先ビーカーをセットして燃料を指定した分だけ移動させる。これは、ETH の送金を指す。

(2) 応用プログラムと初期パラメータを記述した長大なカードとビーカーをセットして、メモリにプログラムを書き込む（デプロイする）。計算機はそのプログラムの初期化のコードも実行して応用プログラムをセットアップする。これは、スマートコントラクトをブロックチェーンに書きこむことを指す。

(3) 短小なカードとビーカーをセットして、メモリ上のプログラムを呼び出して使う。これは、書き込まれているスマートコントラクトを呼びだして使うことを指す。

トランザクションを実行したい人は、自身の「署名記事」として燃料の注入元のビーカーの住所、パンチカードの内容、計算機を動かすバリデータに譲ってもよい燃料の量（優先料金）と、使ってよい燃料の最大量を記したコピー紙をバリデータらに向けてばらまく。実行されたトランザクションの記事がまとめられ、新聞の 1 ページを構成する。

機械式計算機は、一定の燃費で動くのではなく、トランザクションが混み合うと燃料を多く必要とし、空くと燃料が少なく済む。

決められた額の ETH をシステムにデポジットした人はバリデータになる。12 秒間隔の「スロット」で時間が区切られ、各スロットでバリデータの誰かがくじに当たる。当たったバリデータは、集めた記事から実際に実行する分を決めて、計算機を動かし、新聞の 1 ページを構成し提案する。遂行しなければ、そのスロットでは紙面はできなかったことになる。紙面を受け取った他のバリデータは確かめ算をする。この課された仕事を遂行すればデポジットの ETH が増え、遂行しなければデポジットの ETH が没収される。

バリデータは、エポック（32 スロットを 1 エポックとする）のどれかのスロットの担当の委員会（ビーコン委員会）に割り当てられ、そのスロットで提案された紙面の正しさに証言（署名）する。

エポックの先頭のスロットはチェックポイントと呼ばれ、バリデータは、連続するふたつのエポックのチェックポイントに特に証言する。デポジット総額の 3 分の 2 に相当するバリデータからの証言が得られた場合、最新のチェックポイントは正当化され、そのひとつ手前のチェックポイントは確定される。

エポック内の紙面の列に分岐が起きた場合、デポジット換算で一番たくさんの証言を得ている履歴を採用する。コストが一番かかっている履歴が一番正しい。

バリデータとしての役割を遂行し、デポジットが増えることで貰える報酬は、自分のデポジット額に比例し、みんなのデポジット総額の平方根に反比例する。証言が遅れると報酬の額は減る。また、報酬はエポック毎に貰うことができる。

NFT (Non-Fungible Token)編

ファンジブルか、ノン・ファンジブルかを見分ける方法は、券を借りて同じ数量を示す別の券ですぐに返した時、怒られるかどうかである。

例えば、1 万円札は製造番号が違う 1 万円札が返ってきたとしても構わないため、ファンジブル（代替可能)である。

一方で、コンサートのチケットは、数量が同じだとしても座席番号で良し悪しがあるため、ノン・ファンジブル（代替不可能)である。

NFT は概念的に券（チケット）であり、発行元をトラストすることにもとづく。

Ethereum 上に存在しない NFT、つまり、未出庫の NFT が売買されている。「出庫手続き」をしない限り、実際には Ethereum にその NFT を書き込まない。これは、Lazy Minting という手法である。ブロックチェーンに書き込むための Gas 使用料が高いため、このような方法が取られる。Gas 使用料は ETH 建てで払うため ETH が高くなると Gas の相場が高くなる。アプリケーションの側から見ると ETH が安いほうが良いが、ETH が安くなると Ethereum ブロックチェーンが危うくなる。

DAO (Decentralized Autonomous Organization) 編

DAO は分散型自律組織のことである。しかしながら、すべての意思決定を誰からもコントロールされず自律的に行っているとは言えない。実際には他律的に動いている。

スマートコントラクトは呼び出されないと動かない。トークンの持ち分による投票に意思決定を依存している。提案はスマートコントラクトのコードとして書かれており、それを全員が読めることが前提となっている。

可決した提案を実行する(計算資源量を買う)人が決まっているのであれば、その人に拒否権があり実質的な支配者と言える。一方で、誰にでもできるなら真意を難読化した提案を用いて容易に攻撃でき、脆弱な仕組みになる。

トークン化によってすべてが解決するわけではない。他者へのトラストに依らずにトークンは所有できても、トークンが指したり包含したりするものは所有できない。

トークンの所持は証明でき、ブロックチェーンは広義に検閲できないため、誰にも邪魔されずに各自の意思表示はできる。したがって、トークンの所持量に応じた投票は実現できる。しかし、すべての意思決定に対して多数決が適しているわけではない。

未来における貨幣・金融の不在

人と労働を密に結合させすぎている。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。電気係という人を動かす時代からアレクサのような自動システムを動かす時代に変化している。つまり、機械がやればよいことを人が行っている分業社会をどう変化させるかを考えることである。

将来実現する「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)」であり、人間にとって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。

つまりは「分業の終焉」である。労働の変化や欲望の二重の一致が自動化され貨幣が不要な社会になりうる。分業社会が終われば貨幣の仕組みも崩れる。今、消費社会、分業社会をどう創造的に破壊するのだろうかということが問われている。

Q&A

Q1.　世間が Web3 をビジネスチャンスだと考えている状況についての意見はあるか。

A1.　Web3 を定義し直し、対象の内容を変更する必要がある。