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 回目の今回は斉藤賢爾氏（早稲田大学大学院経営管理研究科教授）にご登壇いただいた。斉藤氏からは「金融と技術」の 4 回目として「ブロックチェーンと金融システム」と題して、本来のブロックチェーン技術の捉え方とその真価について語っていただいた。

ブロックチェーンの成り立ちとビットコイン

ブロックチェーンの技術は元々ビットコインを成立させるための要素技術として構築されたものである。ゆえに、本来そこからブロックチェーンだけを取り出して議論することに意味のあるものではない。あくまで送金システムの一部であり、送金以外のことに使う場合は設計そのものを見直す必要がある。今はハイプ・サイクルにおける幻滅期で、ビットコインやブロックチャーンが過剰に注目されることがなくなった。ブロックチェーンに対する万能の幻想がないだけに客観的な議論がしやすい。しかし、世間の注目の有無とは別に、技術は改良され続けることを忘れてはいけない。

ブロックチェーンの特徴

ビットコインは自分が持っているお金を自分が自由に使うことを邪魔させないための技術である。今まではオンラインで送金する際は間に金融機関が入る必要があったが、ダイレクトに送金できるようにする。そのためには支払いの記録が改ざんされていないことを証明しなければならない。送金の記録が覆されたり、捏造されていないことを証明する必要がある。

ブロックチェーンは記録を証明できる仕組みであり、一般的に騒がれていることの多くはインターネットの特徴で、ブロックチェーンの特徴ではない。例えば、機能分散と負荷分散はブロックチェーンの特徴に当てはまらない。合意形成も同様に当てはまらず、コンピューターサイエンスにおけるコンセンサスは冗長化に関わっている。冗長化したものが一致していないと誤りというだけのことであり、人間の合意形成はなされていない。ゼロダウンタイムも真っ赤なウソであり 100%アベイラビリティがあることを指すので間違い (ブロックチェーン外のシステム設計に依存する)。ネットワークが分断されている状況で必ず応答するためには、複製されているデータが一致しているか確認できないので、仮に本当にゼロダウンタイムだとすれば、その場合データの一貫性は損なわれてしまう。

巷で言われていることの多くは誤っている。例えば、スマートコントラクトは「契約」(意思表示の合致が本質要件)ではない。ブロックチェーンでは通常、人間レベルの意思表示の

合致が行われておらず、スマートコントラクトは単にブロックチェーン上にコードと内部状態をもつアプリケーションを指すだけなので、人間レベルで意思表示を合致させるようにアプリケーションをわざわざ作り込まなければ契約を実現することはできない。

今、ブロックチェーンなるものを応用したい人にビットコインやブロックチェーンの仕組みを説明することは YouTuber になりたい人に真空管の説明をすることと類似している。「テレビジョン」という技術で人々がやりたいのが、遠くに映像を送ることで、テレビはそのビジネスモデルを含む実装の一例だとすると、ビットコインというビジネスモデルを含む実装で実現されるのは言わば「レッジャー（台帳）」であり、それでやりたいことは記録が改ざんされていないことの証明である。テレビジョンの最初の要素技術が真空管とすると、レッジャーの最初の要素技術はブロックチェーンが該当する。

デジタル署名によってトランザクションが正常であることは証明できるが、ダブルスペンディングなどの問題はある。ハッシュ関数から出てくるダイジェストがブロックの中身が少しでも異なると全く違う値になる。ダイジェストは手前のブロックから引き継いでいる値より小さくなければならず、計算してみないとその値はわからない。ダイジェストがターゲット以下の値になるまで計算していて、その値になって初めて公表される。ブロックの生成も追い抜かないといけないので改竄が不可能、その改竄自体にも莫大なコストがかかる。

作業証明（Proof of Work）のコストが一番かかっているものを採用することがナカモトコンセンサス。改竄をしようとするとコストがかかるので、作業証明が長いものを使うといった合理的な理由から採用されている。作業証明の場合は投入される電力コストは仮想通貨の市場価値と均衡するが、それはビットコインの価値が高いと電力コストが追従して高くなるし、逆に安いと電力コストも抑えられるという考え方である。ビットコインの仕組みは市場価値に守られているのは弱点といえる。イーサリアムの場合はイーサの上にアプリケーションを載せているため、イーサリアムが暴落して止まるとアプリが動かなくなってしまう。

ブロックチェーンによって実現するもの

遺言書の作成では本人が亡くなる前に本人の秘密鍵として、ハッシュ関数（ダイジェスト）に PDF を埋め込み、ダイジェストの値を確認して本人のものかどうかを確認することが可能になる。オンラインバンキングの通帳データの証拠証券化も同様に CSV ファイルのダイジェストをデジタル署名に埋め込むことで可能にする。

パブリックなブロックチェーンは仮想通貨の価値が高い間はブロックチェーン技術が担保されているが、価格が下がった場合は信頼できない。

今後ブロックチェーン技術によって証明機関を自分で行うことができるようになるし、予約システムのようなものにも使用できるようになる。コンピューターのプログラムコー

ドの保全や契約の自動化など、自動的に動ける基盤が生成される。それによって金融機関の解体にもつながり、自由に貨幣媒介ができるようになる。貨幣に変わるものが裏側で動いてくことは貨幣の消滅にもつながるのではないか。

そうしてサイボーグ社会への変化が起こる。社会が新しい手や足を持つようになり、労働の対価としての貨幣が変化し、欲望と二重の一致が解消されたりする。生産が自動化され、流通が自動化された社会で貨幣の役割はないと思っている。社会の目や耳を通して得た情報は正しいかどうか、自動化の責任の所在がどこにあるのかの制度設計が必要。何が正しいのかを作らなければならない。ビットコインが送金のために作られたように何が解くべき問題なのか。デジタル技術によって消費社会がどうディスラプトされていくのかを考える必要がある。

Q&A

Q.改ざんできないということは誤った入力を修正できないのか。悪意を持った攻撃によってログが汚くなるのか。オフチェーンのところで本当に正しい入力がなされているのか。
A.誤入力があれば記録を残しておけばいい。記録が間違っていたら直す、権限の問題。実用的なところは自動化する。メーカーが公開している公開鍵で証明可能。技術と社会制度などの社会的な証明は行政が行うべき。

Q.プライベート型のブロックチェーンはなぜ取り組む企業があるのか。
A.失礼な言い方をすれば基本的に原理がわかっていないから、より悪いのはわかっていてやっている企業。悪用というかストラテジックに使っている人もいる。

Q.ブロックチェーンは正誤を証明するのかは得意、改ざんされていないことを証明する研究を行っているが、ブロックチェーンは即時性がないことへの解決策はなにがあるのか。キャッシュとしてもっているセカンドレイヤーとのやり取りの際にはブロックチェーン上に記録されないことについてはどう思うか。
A.チェーンでやっていると即時性がないので、セカンドレイヤー部分がバッファリングするやり方と、プライベートな台帳がたくさんあるならそこを利用して普通のトランザクションと同じ仕組みを作る。使うときには使う、初期の段階にはセカンドレイヤーの動き方でもよい。

追加参考書籍

- 杉井靖典『いちばんやさしいブロックチェーンの教本　人気講師が教えるビットコ

インを支える仕組み』2017 インプレス
- Kalle Roenbaum (2019) “Grokking Bitcoin” Manning Publications