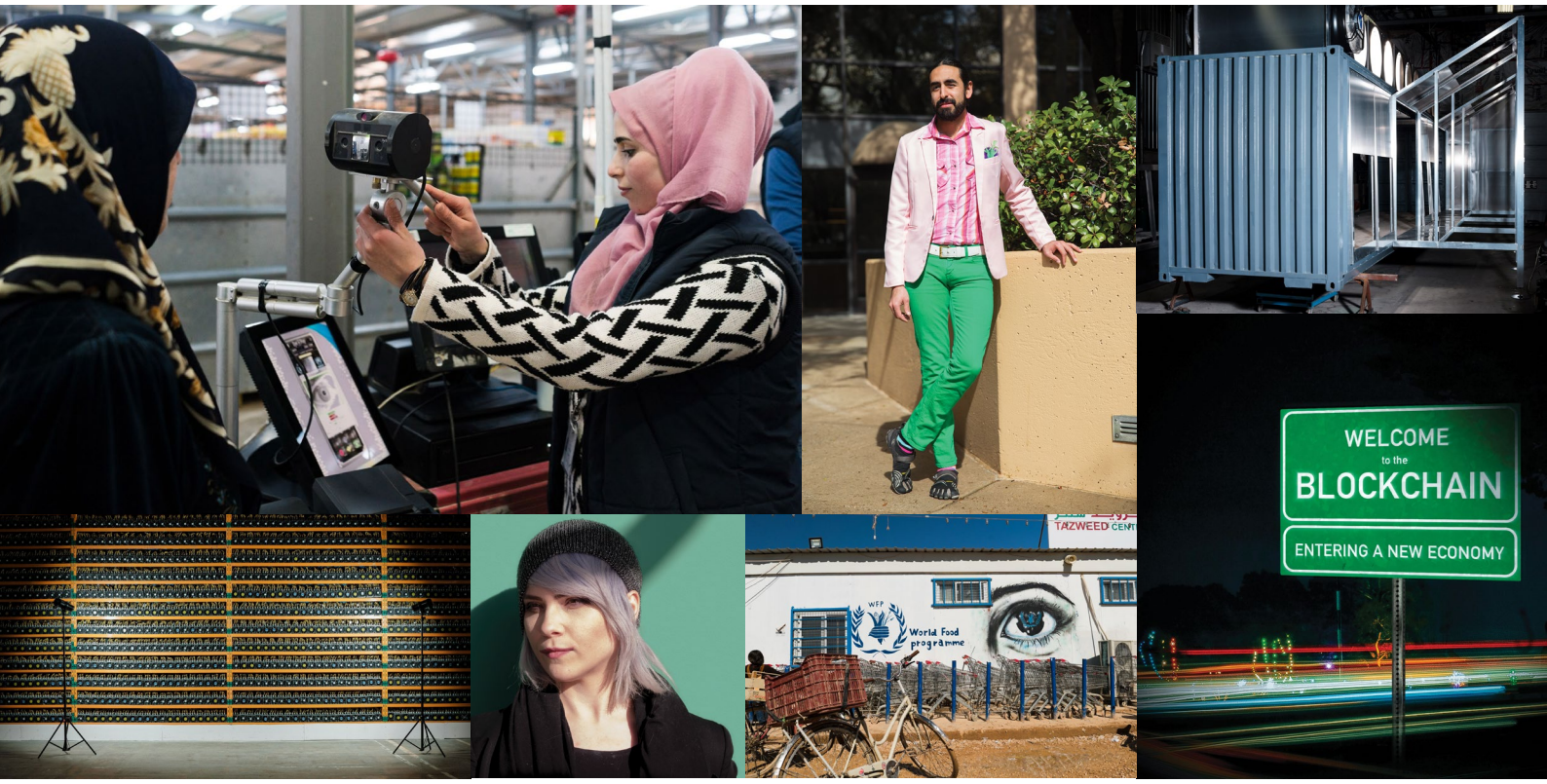
MIT Technology Review
Published by KADOKAWA / ASCII

Blockchain 2

「非中央集権化」の先にあるもの



CONTENTS

「ブロックチェーンはインターネットの再来だ」という人が多い。だが、なぜブロックチェーンが優れているのか？ただの分散データベースとはどう違うのか？ 説明できるだろうか。
今回の e ムックでは、ブロックチェーンの本質である「非中央集権」をさまざまな角度から取り上げた記事を収録した。「信用コスト」に着眼した経済的影響の考察、社会実装における安全性の問題、難民支援における活用の実例まで、ブロックチェーンの先にある「非中央集権型社会」の未来を考えるきっかけとしたい。


WELCOME
to the
BLOCKCHAIN
ENTERING A NEW ECONOMY

複式簿記以来の革命 ブロックチェーンが作る 新しい「信用」

by Paul Vigna

Illust by Selman Design

ブロックチェーン技術を一攫千金やマネー・ロンダリングのためだと考えていると、
将来の非中央集権型経済の基盤としての価値を見逃してしまう。
ブロックチェーン台帳による改編不能な台帳の出現により「信用」に対するコストが大幅に下落し、
不完全な信用の創造で利益を得ている銀行、金融機関、財政アドバイザーたちを脅かすことになる。

1990 年代に異常な勢いで膨れあがったインターネット・バブルは、最終的には数千億ドルもの富が失われて幕を閉じたと一般的には考えられている。バブル時代に低コストで調達した資金で作ったインフラ上に、バブル崩壊後、インターネットのイノベーションが起こったことは、あまり議論されていない。こういった資金は、光ファイバー・ケーブルや 3G ネットワークの研究開発費、巨大サーバー・ファーム（データ・センター）の構築に費やされた。こうして整備されたすべてのインフラによって、アルゴリズム検索やソーシャル・メディア、モバイル・コンピューティング、クラウド・サービス、ビッグデータ解析、人工知能（AI）など、今や世界の最も強力な企業の基盤となっているテクノロジーが実現したのだ。

熱狂的で乱高下が激しい暗号通貨やブロックチェーン・ブームの裏で、インターネット・バブルと同じようなことが起きていると考えられる。2017 年、空前の高値をつけた暗号トークン価格が暴落した時、ブロックチェーン懐疑論者は大喜びで歓声を上げた。だが、彼らは自分たちが馬鹿にしている暗号通貨の投資家と同じ間違いを犯している。内在する価値と価格とを混同しているのだ。ブロックチェーン・テクノロジー上に生まれる「優良産業」がどのようなものになるのか、ま

だ予想できないが、必ず出現すると確信している。なぜならこのテクノロジーが作り出しているのは、「信用」という金銭では買えない貴重な資産だからだ。

優良産業が必ず生まれると信じる理由を説明するには、14 世紀までさかもぼる必要がある。

イタリア人の商人や銀行家の間で複式簿記が使われ始めた頃のことだ。複式簿記はアラビア数字の導入により可能になり、商人は信頼できる帳簿記録法を手に入れ、銀行家たちは国際決済システムの仲介業者として新たに強力な役割を担うようになった。だが、複式簿記は近代金融の道を開いた道具にとどまらなかった。当時の文化に取り込まれていったのだ。

1494 年、カトリック教会フランシスコ会の修道士で数学者のルカ・パチョーリは、金銭の流れを追うためだけでなく道義的責任として、数学と会計学に関するマニュアルを出版し、複式簿記の考えを体系化した。パチョーリがいうには、商人や銀行家は取得した価値の代わりに、何かを返さ

なければならない。つまり、借方は貸方とつり合い、資産は負債と釣り合うといった具合に、お互いを相殺する項目を 2 つに分けて記載するのだ。

それまで軽んじられていた商人たちは、パチョーリの高潔な会計学の登場で宗教的な祝福を受けた。その後の数百年間で、偽りのない帳簿は誠実さと敬虔さのしるしだとみなされるようになり、手形交換所が決済仲介業者に姿を変え、貨幣の流通速度が上がった。このことはルネサンスに資金を供給し、世界を変える資本家が爆発的に増える道筋をつけた。

とはいえ、このシステムでも粉飾されることはあった。銀行家などの金融関係者は、帳簿を誠実に作るという道徳的義務を頻繁に放棄してきた。そして、今も変わらない。史上最大級の巨額詐欺事件の犯人として知られる米実業家バーナード・マドフの顧客や、巨額の粉飾決算が発覚し破綻に追い込まれたエンロン（Enron）の株主ならよく知っているだろう。また、たとえ帳簿に不正はなくとも、それなりの代償を払わなければならない。銀行や証券取引所などの一元的な信託管理人が欠くことのできない存在となり、その他の金融仲介業者は単なる仲介業者からゲートキーパー（企業の財務状況分析や開示情報の精査に携わる専門家や組織）に変貌した。ゲートキーパーは、顧客から手数料を徴収し、顧客を選ぶことで摩擦を生み出してイノベーションを萎縮させ、自らの市場の独占的地位を強固にしている。

では、ブロックチェーン・テクノロジーの何に期待しているかというと、一晩で誰かを億万長者にすることでもなければ、詮索好きな政府から財務活動を隠すことでもない。期待しているのは、会計学に対する徹底的な非中央集権的なアプローチや、ひいては経済団体を組織する新しい方法を作り出すことであり、信用コストを大幅に削減することなのだ。

必要な信用の提供や、そのコスト負担を中間業者に頼ってしまったことが、グーグルやフェイスブック、アマゾンなどの巨大企業が、量的メリットやネットワーク効果に乗じて、事実上独占できた理由の 1 つだ。

新しい形態の簿記など作ったところで、凡庸だと思うかもしれない。だが、紀元前の都市国家バビロンのハンムラビ王までさかのぼること数千年、帳簿はずっと文明の基盤だ。社会の基盤である価値の交換をするには、それぞれの所有物や債権、借金などについてのお互いの主張を信用する必要がある。その信用を獲得するためには、社会全体に取引を常時監視する共通のシステムが必要だ。もしそうでなければ、アマゾンのジェフ・ベゾス CEO が世界一の富豪で、アルゼンチンの GDP は 6 億 2000 万ドルで、人類の 71% が 1 日 10 ドル以下で生活し、アップルの株式が 1 株あたりの利益に対して特定の倍数で取引されていることを、知ることは不可能だろう。

ブロックチェーンの本質とは何か?

ブロックチェーンは、取引をリスト化した電子台帳だ（ブロックチェーンという言葉はよく聞くが、よく誤用もされている）。ここで言う取引とは、基本的になんでもいい。現実の金銭の交換のことでもあり、ビットコインのような暗号通貨の基礎となるブロックチェーン上にあるものでもいい。デジタルの株券のような資産の交換にしるしをつけることもできる。また、株の売買などの注文を記録することにも活用できる。ある条件下で契約をコンピューターで自動化するスマート・コントラクトも、ブロックチェーン技術を活用している。たとえば、株価が 10 ドルを下回ったら購入する、といった具合だ。

ブロックチェーンが特別なのは、銀行や政府機関など単一の団体が「中央集権型」で台帳を管理するのではなく、「非中央集権型」ネットワークとして独立した複数のコンピューターにそれぞれコピーを保管している点だ。台帳を管理する団体は 1 つではない。「コンセンサス・プロトコル」によって指図されたルールに従いさえすれば、ネットワーク上にあるコンピューターならば、どのようなものでも台帳を変更できる。コンセンサス・プロトコルとは、ネットワーク上の他のコンピューターの過半数が変更に合意するよう求める数学的アルゴリズムだ。

このアルゴリズムによって合意が成立すると、ネットワーク上のすべてのコンピューターが同時に台帳のコピーを更新する。合意なしに台帳に記帳しようとしたり、さかのぼって記帳を変更しようとしたりすると、自動的にネットワーク上のコンピューターがその記帳を無効として拒絶する。

通常、取引情報はある一定の大きさのブロックに保存され、合意アルゴリズムによって作られた暗号鍵によって、それぞれのブロックが鎖状につながれる（これが「ブロックチェーン」と呼ばれる所以だ）。このプロセスが、共有された「不変」の「真実」を作り出す。物事が正しく定められていれば、手を加えることのできない記録だ。

この全体的な枠組みの中には、さまざまなものがある。たとえば、多くのコンセンサス・プロトコルがあるが、どの種類の安全性が一番高いかについてはしばしば意見の相違がある。原則的に誰でもコンピューターをつないでネットワークの一部になれる公式の「非許可型（パーミッションレス）」ブロックチェーン台帳がある。非許可型ブロックチェーン台帳はビットコインやほかの暗号通貨のほとんどが属している組み合わせだ。また、暗号通貨をまったく使わない非公式の「許可型（パーミッション）」台帳システムもある。これらは一部の組織・団体で使われるかもしれないが、こうした組織・団体は、一般的な記録システムを必要しているもののお互いは独立しており、おそらく完全にお互いを信用しているわけではない。たとえば、製造業者と部品供給業者などがそうだ。

これらすべてに共通しているのは、数学的規則や鉄壁の暗号は、誤りを犯しがちな人間や組織に対する信用よりは、台帳の清廉性を保証するために使われているということだ。これは、暗号作成者のイアン・グリッグが「三式簿記」と称したもので、借方ともう片方の貸方に記帳後、3 番目に不変で明瞭な共有台帳に記帳する。

無視される中央集権型の信用コスト

非中央集権型モデルのメリットは、現在の経済システムの信用コストを計ると分かる。たと

えば 2007 年、リーマン・ブラザーズは最高収入および最高利益をあげていた。財務はすべて会計監査法人のアーンスト・アンド・ヤング（Ernst & Young）の監査を受けていた。だが 9 カ月後、リーマン・ブラザーズの資産価値は急落し、158 年間続いた老舗企業は倒産、過去 80 年で最大の金融危機を引き起こした。それまで帳簿に記されていた評価が、完全に間違っていたのは明らかだ。また後に分かったことだが、リーマンの台帳だけが疑わしいデータを記帳していたわけではなかった。欧米の銀行も、粉飾したバランスシートが原因で生じた損失を補填するために、罰金や返済に数千億ドルを支払った。リーマン・ショックにより、中央集権型組織が内部的に作り上げた数字をそのまま信用すると多額の代償を払わされることが分かった。

リーマンの件は信用コストの極端な例だ。だが、信用コストが経済の他の分野に深く浸透していることも分かった。世界中の高層ビルの個室を埋め尽くす会計士たちを考えてみよう。企業と取引先

相手はどちらも相手の記録を「信用」していないために、会計士は顧客企業の台帳を取引相手の台帳とつじつまを合わせることで、彼らの仕事は成り立っている。時間もコストもかかるが、必要な作業だ。

他に信用コストで明らかなのは、できることではなく、できないことにある。20 億もの人が、資産内容や素性が銀行に信用されないという理由で、口座が持てずに世界経済から閉め出されている。一方で、数十億の自律型デバイスの組み合わせで新しい効率を作り出す、モノのインターネット（IoT）は、装置から装置への微少なやり取りを管理する中央集権型台帳の仲介コストがかさめば実現しないだろう。こういった問題がイノベーションを制限している例は他にも多数ある。

経済の専門家はこういったコストをほとんど認識してないし、分析もしていない。おそらく、会計調整などの業務が不可避でビジネスに必要不可欠な機能だと決めつけている（インターネット時代以前のビジネスでは、毎月の請求書を送るのに莫大な郵送費を支払うしかないと考えられていたように）。この盲点が、なぜ一部の卓越した経済学者がブロックチェーン・テクノロジーをすぐに却下したのかを説明しているかもしれない。多くの人は、ブロックチェーン・テクノロジーにかかるコストを正当化できないという。だが、そういった分析の多くは、新しいモデルが克服しようとしている多大な社会的信用コストを計っていない。

しかし、ブロックチェーンを活用する人は増加している。2009 年 1 月にビットコインがひっそりと発表されると、ビットコインの支持者は、過激な自由意志論者、元ウォール街の専門家、シリコンバレーの技術者、世界銀行などの機関からの開発支援エキスパートまで膨れあがった。多くの人はブロックチェーン・テクノロジーの登場を、インターネット経済における必要不可欠な新しい段階として見ている。間違いなく、初期のころに比べてブロックチェーンに対する認識は変化したといえる。インターネット初期の混乱期では、リーンなデジタル仲介業者がリアル・ビジネスを襲ったのに対し、今回の動きは営利目的の中間業者全体のあらゆるアイデアに挑んでいる。

必要な信用の提供や、そのコスト負担を中間業者に頼ってしまったことが、グーグルやフェイスブック、アマゾンなどの巨大企業が、量的メリットやネットワーク効果に乗じて、事実上独占できた理由の1つだ。事実上、こういった巨大企業は中央集権的に台帳を管理して、おそらく世界で最も重要な「通貨」とされている大量の「取引」記録、つまり私たちのデジタルデータを積み上げている。こういった記録を管理することで、巨大企業は私たちを管理しているのだ。

コードが自由に手に入るようになると、未来の非中央集権型経済が作られる基礎となる。

強固な中央集権的システムを打ち負かすには、激しく乱高下しながら価格が上昇するゴールド・ラッシュのような暗号トークン市場の裏にある重要な要素が必要だ。多くの（おそらくほとんどの）投資家はただ短期で儲けたいと思っているだけで、なぜテクノロジーが重要かとは考えていないことは明らかだ。だが、こういった狂乱は、理性を失っても、いきなり冷めたりしない。たとえば、鉄道や電力といった変化を作り出してきたこれまでのプラットホーム技術のように、さまざまな憶測が飛び交うのはほぼ避けられない。なぜなら、すばらしい考えが新しく登場するときは、それがどれだけの価値を生み出すのか、破壊するのか、そしてどの企業が勝ち、どの企業が負けるのかを予想する枠組みが、投資家にはないからだ。

ブロックチェーンが客観的真実を記録・蓄積できるように、さらに堅牢なシステムとしてできあがる前に、克服しなければならない大きな障害はすでに現場で試されている。

IBM やフォックスコン（Foxconn）などの企業は、貿易金融の解禁や、サプライチェーンの透明性を高めるプロジェクトでデータの不変性の概念を探究している。また、透明性が高まることにより消費者が購入商品に関するより良い情報を得られるようになる。たとえば、あるTシャツが搾取労働で作られたか否かなどだ。

もう1つの新しい重要な考えは、「デジタル資産」についてだ。ビットコインが登場する前は、