# ブロックチェーンの現状と今後

山崎 重一郎 ●近畿大学

**FinTechの中核技術として金融機関や政府による投資と実証実験が盛ん。法整備や標準化も始まる。技術的課題への対策としてオフチェーン技術が注目される。**

## ■ブロックチェーン技術の担い手の交代

ブロックチェーンや仮想通貨に関する状況は、この1年で大きく変化した。中でも重要な変化は主たる担い手の交代である。

ビットコインなどの仮想通貨の開発や運営そして普及活動の担い手は、当初、政府や国家による管理を嫌うリバタリアン的志向を持つ「ビットコイナー」と呼ばれる人達であった。ビットコインの発明者であるサトシ・ナカモト（偽名）も、メーリングリストのログなどによると、そのような思想的志向を持つ人物であった。

しかし近年では、リバタリアンとは正反対とも言える、金融機関やIT産業、中央銀行、政府機関などが、ブロックチェーンや仮想通貨に対する研究開発や実証実験の主役になった。その理由は、ブロックチェーンや仮想通貨が金融とITの融合を意味する「FinTech」の中核技術と目されるようになったからである。FinTechに対する投資は、アメリカ、イギリス、中国を中心に100億ドルにのぼると言われ、莫大な金額の投資が世界各地で行われるようになっている。

日本でも世界に少し遅れるが状況は大きく変化した。日本を代表する3つのメガバンク（三菱東京UFJ銀行、みずほ銀行、三井住友銀行）がブロックチェーンの共同研究や実証実験の計画を発表したほか、業界団体である全国銀行協会も「ブロックチェーン技術の活用可能性と課題に関する検討会」を設置した。

また、日本銀行や複数の省庁も制度設計や標準化などの取り組みを開始した。2016年4月に日本銀行にFinTechセンターが設立され、日本銀行主催のFinTech勉強会として、技術、法律、経済の分野の有識者からなるブロックチェーン技術の検討が行われている。2016年5月には、経済産業省から「ブロックチェーン技術を利用したサービスに関する国内外動向調査」というレポートが公開された。

## ■ブロックチェーンや仮想通貨の実証実験

イギリスの中央銀行であるイングランド銀行は、中央銀行のためのブロックチェーンと仮想通貨の研究開発を行っていることを、2016年2月にサンディエゴで開催されたNetwork & Distributed System Security（NDSS）シンポジウムで発表した。ロンドン大学などとの共同による「RSCoin」である。

ゴールドマン・サックスやBNYメロン、UBS、JPモルガンなど世界の著名な銀行や、日本のメガバンクを含む42行をメンバーとするブロック

チェーンのコンソーシアムが「R3CEV」である。2015年から実証実験を行っていたが、2016年4月にCordaという独自のブロックチェーンシステムを開発していることを発表した。

JPX（日本取引所グループ）は、ブロックチェーン技術の金融分野への適用に関する大規模な実証実験を行い、その成果を2016年8月に「金融市場インフラに対する分散型台帳技術の適用可能性について」というレポートとして日本語と英語で公開した。

また仮想通貨についても、2016年7月に三菱東京UFJ銀行が、「MUFGコイン」という仮想通貨を開発していることを公表した。ほかにも三菱東京UFJ銀行については、世界最大の仮想通貨取引所を運営する米コインベースに出資してパートナーシップを締結することを発表するなどの動きもあった。

## ■学術研究の動き

ブロックチェーンや仮想通貨に関する学術研究は、2013年ごろから行われてきたが、2016年には本格的な国際会議が多数開催されるようになった。

2016年2月にカリブ海のバルバドスで開催された20年の歴史を持つ金融暗号の国際学会Financial Cryptography and Data Securityでは、Bitcoinのワークショップが開催され、スタンフォード大やロンドン大学などが研究成果を発表した。また2016年6月には、IACR（国際暗号研究学会）のBitcoinの国際ワークショップがギリシャのコルフ島で開催された。

これら以外にも数多くの国際的な学術シンポジウムやワークショップが開催されている。

## ■仮想通貨への法制度の整備状況

2015年6月に開催された主要国首脳会議（エルマウ・サミット）の宣言に、仮想通貨の管理が盛り込まれた。これを受けて金融活動作業部会（FATF）から、仮想通貨によるテロリストへの資金供与や、組織犯罪、野生動植物の違法取引の防止を目的に、仮想通貨と法定通貨の交換所の登録・免許制、顧客の本人確認や、怪しい取引履歴の届け出、保存義務などを内容とする報告書が公表された。

以前よりアメリカやEUにおける金融当局の国際的規制として、金融機関におけるマネーロンダリングによる犯罪収益移転を防止するために、「ノウ・ユア・カスタマールール（KYC）」が定められていた。これと同様のルールが、主要国の仮想通貨の交換所にも適用されることになった。

わが国でも、2016年5月の伊勢志摩サミットの直前に、「情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律案」が成立した。これらの法整備により仮想通貨を適正に、そして自由に利用するための国際的な環境が一応は整備されてきたといえる。

## ■ブロックチェーン標準化の動き

2015年には、金融技術の標準化を担うISO/TC68に、デジタルカレンシーの通貨記号に関する標準化を扱うSC7サブグループが設置された。

またオーストラリアから、ブロックチェーン技術の標準化に関する新たなTCの設立が提案され、2016年9月にISO/TC307 Blockchain and electronic distributed ledger technologiesが設立された。このTCのParticipating memberは、日本、オーストラリア、カナダ、中国、デンマーク、フィンランド、フランス、ドイツ、イタリア、韓国、マレーシア、ノルウェー、イギリスである。これを受けて、2016年10月に国内でも経済産業省の外郭団体のJIPDECにISO/TC307に係る国内審議団体が設置された。

## ■ブロックチェーンの定義の混乱

莫大な資金の流入による熱狂の渦中にあることが、「ブロックチェーン」という用語が甚だしく拡大解釈される要因になっている。さらに、関連して「分散台帳」という用語も登場するようになった。IBMが中心となって開発が進められているオープンソースHyperledgerでは、ブロックチェーンではなく分散台帳と呼んでいる。

また、「ブロックチェーン」という用語の内容が未定義なまま、「通貨以外の用途にも広範に利用可能な革命的な技術だ」という言説が広まっている。その期待と投資に呼応してブロックチェーンと称するシステムが次々に登場している。ブロックチェーンという用語の正確な定義が存在しないために、ブロックチェーンと自称している技術が何を指しているのか不明である。現在、異常なまでに膨張している幻想のバブルが弾け、幻滅期が到来する可能性を否定できない。

## ■ビットコインのブロックチェーン

ビットコインの発明者のサトシ・ナカモトの論文によると、ビットコインの開発目的は「信頼できる第三者」を必要としない通貨システムの提案である。そしてブロックチェーンは仮想通貨ビットコインの中核となる台帳システムとして発明された。

電子通貨の最大の課題は、電子通貨の二重使用の問題である。従来はこの問題の解決には、ICカードなどの特殊なハードウェアや信頼できるサーバが必要だと考えられていた。これをビットコインは、世界中の夥しい数の仮想通貨利用者によって構成されるP2P型ネットワークのすべてのノードが、ブロックチェーンによる取引台帳の整合性監査を定常的に繰り返すことによって、電子通貨の二重使用の問題をソフトウェアだけで鮮やかに解決した。

## ■対称的な非集中型の台帳監査システム

ビットコインのP2P型ネットワークのノードはすべて対等で、特別なものは一つも存在しない。つまり、ビットコインのブロックチェーンは完全に対称的な非集中型（decentralized）の台帳監査システムである。

またビットコインでは、通貨発行益をめぐるゴールドラッシュに似た人々の欲望に基づく計算競争（マイニング）が常態となるよう巧妙に設計されている。この競争に勝利するためには消費電力が問題となるほどの莫大な計算が必要である。

この競争状態は、仮想通貨システムにおいて3つの重要な機能を担っている。その1つ目は、仮想通貨経済圏における通貨発行手段となっていることである。

2つ目は、地球全体に広がる大規模な分散台帳システムにおいて、世界各地で非同期に発生する台帳記録を時系列的に一貫したものになるよう、マイニング競争によって生じる一種の確率的な選択の繰り返しによって最終的に記録内容を一意に合意するための手段になっていることである。

3つ目は、この計算競争が結果として、ビットコインのブロックチェーンの台帳記録を、いかなる人や組織にも書き戻すことができない非可逆的記録にしているということである。なぜなら、一旦書き込まれた台帳記録を後で書き換えるためには、マイニング競争の計算結果を再計算し、さらに一定期間マイニング競争に連続して勝利する必要があるが、それは現実には不可能だからである。

これらは技術的な仕組みだけで実現されているわけではない。ビットコインが仮想通貨として現実に価値を持ち、それを求めて膨大な計算を行い続けているマイナーの存在が不可欠である。

## ■ブロックチェーンの絶対中立性

「ザ・ブロックチェーン」すなわちビットコインのブロックチェーンは、人が創りだしたものでありながら、人には支配できないシステムである。ザ・ブロックチェーンの記録は、国家や大企業などを含めて、特定の人や組織には絶対に支配できない中立的な非可逆的記録である。

ザ・ブロックチェーンは、人ではなく「Code」（プログラムと法の二つの意味を持つ）が支配している。すべてのノードが「Code」の仕様にそって台帳記録の検証を行うからである。絶対中立的なシステムの運用方法の知見は少ない。たとえば、「Code」そのもののガバナンスの方法もその一つである。現時点では手探りの段階ながら確実に前進していると言ってよいだろう。

## ■非可逆的記録としてのブロックチェーン

この絶対中立的な非可逆的記録という性質は、他の「ブロックチェーン」では自明ではない。

たとえば、仮想通貨Ethereumでは、2016年6月にThe DAOというEthereum上のクラウドファンディングプラットフォームからの資金流失事件が発生し、被害者らの圧力によって、Ethereumのブロックチェーンを事件発生以前の時点にまで書き戻した。これを実施したのは、Ethereumの発明者であり主要な開発者でもあるVitalik Buterin氏である。この事実により、Ethereumのブロックチェーンは、絶対中立的な非可逆的記録ではないことがわかる。

## ■ブロックチェーンの今後

FinTechの主役として過熱しているブロックチェーンへの期待は、短期間に実現するものではないが、幻滅期に入っても消え去ることはないだろう。現在のブロックチェーン技術は玩具レベルだが、実用技術に昇華するための技術革新は次々に提案されて実施されている。また、「ブロックチェーン化」は、歴史的理由によって過剰に複雑化している現在の金融システムを刷新する契機になるかもしれない。

ここでは、FinTech以外の用途へのブロックチェーン利用の可能性について触れておく。ただし、これらもやはり短期間で実現するものではない。

### （1）著作権管理の基盤としてのブロックチェーン

これまでの歴史の中で、著作権とテクノロジーは、常に対立関係にあった。新しいテクノロジーの発明は、著作権者やコンテンツ産業の権利に対する脅威を引き起こしていた。新しいテクノロジーの発明、たとえば、レコードやラジオ、録音テープ、家庭用ビデオ、デジタル録音、インターネット、Web、P2P型ファイル共有技術などのテクノロジーの進歩の歴史は、それに対する著作権や著作隣接権の歴史でもあったと言ってよい。

これに対して、ブロックチェーンは著作権や著作隣接権と対立するのではなく、むしろその管理を容易にする技術となる可能性を持っている。ブロックチェーンは、電子通貨の二重使用問題を解決し、デジタルデータの通貨をあたかも現物のコインのように人から人へと安全に転々流通させることを可能にした。これと同様のことをデジタルコンテンツに適用できる可能性がある。ブロックチェーンによる著作権管理は、人間の支配を超えた絶対中立性を持つ。つまり、たとえばJASRAC（日本著作権協会）のような存在がなくても、きめ細かく著作権者に著作権使用料を支払う仕組みを構築できるのである。

### （2）投票の基盤としてのブロックチェーン

紙による投票の開票作業や集計作業では、原理

的に、担当者による不正の可能性を完全に払拭できない。電子投票の場合は、さらに開発や運用の主体による不正の可能性が存在する。電子投票には、電子通貨以上に政府からの中立性と透明性が求められる。

ビットコインは、国家を超越した通貨システムを実現したが、ブロックチェーンは政府や国家を超越した、高度な中立性を備えた投票システムを実現できる可能性がある。

### ■ブロックチェーンの技術的課題への取り組み

ビットコインのブロックチェーンには、時間あたりの取引数に関するスケーラビリティの問題が存在する。また、送金に利用されているアドレスと本人が紐づくと取引の履歴が完全に追跡できてしまうという問題も存在する。

現時点でこれらの問題に対する対策として注目されているのは、ブロックチェーンの外側での決済を可能にする「オフチェーン技術」である。中でも「マイクロペイメントチャンネル」や「ライトニングネットワーク」という提案が有望視されている。また、ビットコインとは別の独自のブロックチェーンと、ビットコインのブロックチェーンの仮想通貨を、双方向でペグ（紐づけ）して連携する「サイドチェーン技術」というアプローチも存在する。

ブロックチェーン技術を玩具レベルから実用レベルに進化させるにはまだ数年の時間が必要だろう。しかし、それはおそらく可能である。

# ［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2017年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先　株式会社インプレスR&D　✉ iwp-info@impress.co.jp