ブロックチェーンへの期待

前川 徹（まえがわ・とおる）

国際大学 GLOCOM 所長

インターネットとの類似性

ブロックチェーンは，仮想通貨であるビットコインの中核技術としてサトシ・ナカモト（Satoshi Nakamoto）氏によって考案された技術であるが，その実態はネットワーク上で「分散型台帳」を実現する技術である．台帳だと考えれば，仮想通貨以外への利用も可能である．すでに株式や債権，投資信託，保険，年金などの様々な金融資産，あるいは不動産登記や自動車の登録，特許や商標といった有形無形の資産，運転免許やパスポートなどの ID への利用可能性が示されている．

こうした利用範囲が広いことに加え，ブロックチェーンの設計思想とアーキテクチャが分散型でありかつオープンである点に注目したい．すでに何人もの専門家が指摘しているように，このブロックチェーンがもつ特徴はインターネットの基本的なアーキテクチャに通じるところがある．インターネットは一つのノードが故障しても，ネットワークの機能は維持されるように設計されている．同じようにブロックチェーンの場合も複数のノードがブロックチェーン全体の情報を保持しているため，一部のノードが機能しなくなってもブロックチェーンの機能は維持される．また，どちらも分散かつ自律的なシステムであるため，拡張性，成長性に優れている．

ただし，インターネットに比べるとさらに複雑な理論と仕組みで成り立っているため，多くの人にとって，ブロックチェーンは理解し難い技術になっている．それが証拠にインターネット上にはブロックチェーンの仕組みをわかりやすく解説するというコンテンツがたくさんある．この難解さがブロックチェーン普及の

前川 徹
国際大学 GLOCOM 所長．1978 年通商産業省入省，94 ～ 97 年日本貿易振興会（JETRO）ニューヨークセンターの産業用電子機器部長時代に米国の情報産業とインターネットの動向に関するレポートのネット配信を行う．情報処理振興事業協会（IPA）の技術センター所長（兼セキュリティセンター所長），早稲田大学大学院国際情報通信研究科客員教授，（株）富士通総研経済研究所主任研究員，（一社）コンピュータソフトウェア協会専務理事を歴任（組織名はいずれも当時）．未踏事業の提案者．サイバー大学 IT 総合学部教授などを兼務．

障害の一要因になるかもしれない．ただ，私はこの点については楽観的である．

魔法と区別できない技術

人は理解できないものや理解の範囲外にあるものに対して，嫌悪感や恐怖を覚えて排斥する傾向がある．しかし，技術に関しては，時間とともに人は恐怖や嫌悪感を忘れて寛容になる．SF 作家のアーサー・C・クラーク（Arthur C. Clarke）は「高度に発展した科学技術は魔法と区別がつかない」と述べたと言われているが，我々はすでに半世紀前の時代に生きた人からみれば魔法としか思えない技術に取り囲まれて生活している．特に，その仕組みが目に見えないソフトウェアは直感的な理解が困難で，多くの人にとっては魔法に等しい．たとえば，ネットショッピングでは当たり前のように利用されている SSL（Secure Sockets Layer）は，通信相手が信頼できることを確認したうえでデータを暗号化して送受信する仕組み（プロトコル）であり，これによって，私たちは個人情報やクレジットカード情報などをサーバに送ることができるのだが，その仕組みをきちんと理解している人はそれほど多くない．通信を暗号化するための共通鍵を，公開鍵暗号を利用して交換するという仕組みは知っていても，公開鍵暗号の仕組みまできちんと理解できている人はかなり少ないのではないだろうか．それでも多くのインターネット利用者は，SSL を利用してネットショッピングを行っている．それは多くの人にとって魔法と同じようなものになっている．SSL という呪文さえ唱えておけば情報は守られるうえに，その魔法の呪文すら自動的に唱える仕組みになっている．

信頼性に対する不安の問題

もし，普及の障害になるものがあるとすれば，ブロックチェーンの信頼性に対する不安かもしれない．ビットコインや類似の仮想通貨を巡ってはいくつもの事件が起きている．たとえば，2014 年 2 月には当時世界最大のビットコイン取引所マウントゴックス（MTGOX）社が破綻しており，その引き金を引いたのは，顧客から預かっている約 75 万ビットコインと現金 28 億円が紛失した事件である．当初は外部からのサイバー攻撃によって起きたと報道されたが，翌年の 9 月に同社の代表取締役であるカルプレス・マルク・マリ・ロベート（Mark Marie Robert Karpelès）が私電磁的記録不正作出・同供用罪及び業務上横領罪の容疑で起訴されており，経営者による業務横領の可能性もある★1．

また，2016 年 6 月にはイーサリアムの技術を利用してつくられた「The DAO」というスマート・コントラクト・プロジェクト内で不正送金が行われたという事件が発生しているほか，同年 8 月には香港のビットコイン取引所ビットフィネックス（Bitfinex）で約 12 万ビットコインが盗まれるという事件も起きている．

こうした事件を耳にすると，一般のネット利用者は，ブロックチェーンの信頼性に何か問題があるのではないかと不安に感じるだろう．その不安がブロックチェーンの普及の障害になる可能性がある．しかし，これらの事件はビットコインが破綻したものでもなければ，ブロックチェーンに内在する脆弱性が原因で起きたものでもない．

ちなみに，この原稿を書いている時点でビットコインの時価総額は 2 兆円を超えているが，もしブロックチェーンに技術的問題があるのであれば，凄腕のハッカーがこの 2 兆円を見過ごすはずはない．つまり，2 兆円の時価総額はビットコイン，あるいはその中核技術であるブロックチェーンに対する信頼の証なのである．

先見の明

正確な月日は覚えていないが，1993 年の終わりか 94 年の初めに東京大学大型計算機センター教授であった石田晴久先生★2 の講演を聞いた．テーマはイン

ターネットの現状と未来だったと思う．その中で石田先生は「いずれ企業はインターネット上で商取引を行うようになる」と断言された．ネットワークを使った企業間取引はEDI（Electronic Data Interchange）と呼ばれ，主に専用線を使って行われていた時代である．インターネット上のEC（Electronic Commerce）ブームが始まるずっと前で，そもそもインターネット・ブームすら起きていなかった．聴衆のほとんどは，石田先生の予言を絵空事として無視したに違いない．通商産業省（当時）でインターネットの普及活動をしていた私でさえ，ベストエフォート型のネットワークであるインターネットを企業が商取引のために利用するのは難しいと思っていた．しかし，石田先生の予言は正しかった．

ブロックチェーン技術は，ちょうど1990年代前半のインターネットのような段階にある．現時点では，それを自由自在に利用できるのはその技術に長けた一部の専門家に限定されている．しかし，そう遠くなく誰もが簡単に利用できるようになり，多くの人が様々な場面で日常的に利用する技術になるのではないだろうか．

ブロックチェーンは，既存の枯れた技術の組み合わせではあるものの，実によくできた仕組みである．ブロックチェーンを使えば，信頼できる中立的な中央機関がなくても，信頼できる取引台帳を作ることができる．それは，ネットワークにつながったコンピュータが集合的に取引を検証してから，その取引記録を作成し，みんなで承認するという手順（プロトコル）によって実現される．その台帳は，どんなユーザーでも改ざんできず，誰でもその正当性を確かめることができる．それは公開鍵暗号やハッシュによって保障されている．

インターネットが通信ネットワークに革命をもたらしたように，ブロックチェーンはデータベースに革命をもたらす．石田先生にならって言えば，そう遠くない未来，私たちはブロックチェーンという魔法に支えられた利便性の高い様々な仕組みを利用することになるだろう．

註

★1――同社の破産管財人の2016年9月28日付けの報告書によれば，まだ事件の全容は解明されていない．<https://www.mtgox.com/img/pdf/20160928_report.pdf>

★2――1997年に東京大学を退官．多摩美術大学情報デザイン学科教授・メディアセンター所

長を経て，2007 年サイバー大学の IT 総合学部長に就任．2009 年 3 月没．