■レポート■

ブロックチェーンのビジネス応用について

森・濱田松本法律事務所 パートナー弁護士
増島　雅和

1．はじめに

FinTechの流行とともにブロックチェーンに対して大きな注目が集まっている。ブロックチェーンは、もともと仮想通貨のビットコインを実装するためのテクノロジーとして誕生したものであるが、近時、そのテクノロジー自体の有用性が評価され、FinTech分野にとどまらず、流通や製造、公共機関、医療など様々な分野での利用が検討され始めている。他方において、ブロックチェーンが本格的に普及するためには、解決しなければならない数々の課題があることも明らかになりつつある。

本稿は、ブロックチェーンについて概観しつつ、その特性と限界を踏まえた産業における応用の可能性について、現時点における筆者の理解に基づき読者と共有することを試みるものである。なお、ブロックチェーンはまだ技術的には初期の段階にあるテクノロジーであり、テクノロジーの進歩には終わるところがないことから、本稿は現時点における技術水準をもとにした検討に過ぎない。また、ブロックチェーンは現在、世界の各地で集中的な検証・開発が行われており、その中には非公開のものも多く、また公になっているものについてもその全てを網羅して検討することは筆者の認知能力の限界を超える。したがって、本稿はあくまで、現時点で筆者が認識・理解している範囲での検討にとどまること

〈目　次〉

にご留意いただきたい。

2．ブロックチェーンの基礎

本稿はブロックチェーンに関する基礎的な理解があることを前提に、その特性と限界を踏まえた産業における応用の可能性について、構造的に検討することを目的とするものであるため、ブロックチェーンの出自やその技術的な側面に深入りすることはせず、最低限の紹介に留める。

ブロックチェーンは、暗号技術者が情報交換する米国のメーリングリストにおいて、Satoshi Nakamotoと名乗る人物が、2008年11月に公表した論文（注1）をもとに実装されたビットコインの基幹となるテクノロジーである。ビットコインは、2009年に運用が開始されて以降、現在に至るまで一度もシステムが停止したことはなく、2016年２月現在、発行総額にして時価約7,000億円程度の経済圏を全世界に展開することに成功している。

ビットコインとは、ビットコイン・ブロックチェーンの上で機能する仮想通貨アプリケーションである。ブロックチェーンは、ハッシュと呼ばれる元データを要約する技術、公開鍵暗号と呼ばれる暗号技術、Ｐ２Ｐと呼ばれるノード（コンピュータの端末）同士が対等の関係でデータのやりとりを行うネットワーク技術、生成されたチェーンの一貫性を保つための技術（ビットコイン・ブロックチェーンにおいては「Proof of Work」と呼ばれている。）が組み合わされて構成されたものであり、これ自体は純粋な技術の組み合わせとして理解すべきものである。そして、構成される個々の技術に具体的にどのような技術を用いるかによって、様々なブロックチェーンを創作できる。仮想通貨としてのビットコインが実装されているブロックチェーンは、ビットコイン・ブロックチェーンであり、これはブロックチェーンの起源といえる。現在のところ、ノード参加者すなわちネットワークの厚みの上で他の追随を許さないThe Blockchainとでもいうべきものではあるが、ブロックチェーンはこれにとどまるものではなく、様々な仕様のものがありうる。このような多様なブロックチェーンがありうる中でのビットコイン・ブロックチェーンという関係性は、様々な技術仕様のインターネットがある中で、我々が日常用いているインターネットがThe Internetとしての地位を獲得しているのと類似している。

3．ブロックチェーンの類型

ブロックチェーンにおいては、取引をひとかたまりのブロックと見て、一定の承認作業によって承認されたブロックをチェーン状につなげていく。各ノードのチェーンは同期されており、ノード間のチェーンに差違が生じた場合には、一定のルールに基づいた多数決によって正統なチェーンを決定することにより、チェーンの同期を確保していくこととし

ている。

このように、取引の承認作業を分散型の合意形成技術により実現する点にブロックチェーンの特徴があり、これは、各ノードの中に他のノードと異なる権限を持つ者が存在しないという状態を確保することで威力が発揮される（注２）。すなわち、ノードが開放されており、悪意のあるノードが入り込んだとしても、システムが信頼性を保って機能することがブロックチェーンの特徴といえる。

この特徴を確保するために、ビットコイン・ブロックチェーンにおいては、Proof of Workという一連の合意形成作業を行う。これは、あるブロックに任意の値を加えてハッシュの計算を行い、一定の条件を満たす値が得られるまでこの任意の値を入れ替えて計算を実施、条件を満たす値を導き出した場合には、各ノードにおいてこれが正解であることが確認される。この確認がなされると、その計算の集合が新たなブロックとして認定されることになる。この方式の場合、同時に競合する複数のブロックが出現することになる（いわゆるソフトフォーク）が、その中ではチェーンが長い方が正統と評価される。

このように、ブロックチェーンの特徴は、ノードの信頼性を問わずに合意形成を実現するという点にあるが（Trustless）、これを実現するためにスループット（単位時間あたりの処理能力）が犠牲にされる側面がある。世の中の決済取引の中には、決済スピードが重要なものがあり、特に金融における決済システムは、いずれも秒間決済回数が相当程度の大きさであることが必要であることからすると、このパフォーマンスの悪さは商用において時として致命的と評価されかねない。

また、商用のブロックチェーンにおいては、誰でもノードになることができる開放性という特徴は、セキュリティの観点からは必ずしもポジティブに評価されないのが実態である。むしろネットワークを管理下に置きつつ、高スループットを実現することができるのであれば、そのほうが望ましいと考える応用分野も存在する。

Proof of Workが実現しようとする課題は、台帳の改竄や資産の二重譲渡といった通例的ではない事態が生じ、競合する複数のブロックが生じたときに、いずれのチェーンを正統とみなすかという問題であり、ノードの構成員となることができる者をコントロールすることによって、このプルーフ作業を軽減したブロックチェーンの実装があっても良いのではないかという発想が出てくる。これがノードの信頼性を前提とした（Trusted）ブロックチェーンである。

誰もがノードとなることができるということは、すなわちそのブロックチェーンのネットワークは管理者が存在しなくても機能するということを意味し、そのようなTrustlessなブロックチェーンをパブリック・ブロックチェーンという。

これに対し、ノードとなる者を選定することができるブロックチェーンの中には、ブロ

ックチェーンの管理者が単独の者であるプライベート・ブロックチェーン、複数の管理者から構成されるコンソーシアム型ブロックチェーンがある。ブロックチェーンをパブリックなものとして運用するか、プライベートないしコンソーシアムで運用するかは、ブロックチェーンの運用における相違であるともいえる。

しかしながら、他方において、運用に際して悪意のノードの存在をどの程度想定する必要があるか、また分散型の合意形成のために必要なノードのインセンティブ設計をどのように行うか、といった点で、実際にノードとなる者の構成（Trustlessなものとするか Trustedなものとするか）の想定は重要であると考えられる。

4．構成技術とブロックチェーンの特性の関係

前述のとおり、ブロックチェーンは複数の技術の組み合わせによって成り立っているため、ブロックチェーンの特性を理解するためには、構成技術の特性との関連性を理解することが有用と思われる。ここでは、ブロックチェーンを構成する技術を、公開鍵暗号方式を用いた電子署名技術、P2P技術、及び分散型合意形成技術に分けて、それぞれの組み合わせが実現する特性について検討する。

(1) 電子署名技術と分散型合意形成技術

電子署名技術は、取引当事者の真正性（なりすましがないこと）を確保する技術であるが、これとProof of Workなどの分散型合意形成技術を組み合わせることによってコンセンサスを得たデータをチェーン上につなげることができることで、転々流通取引の追跡と検証が可能になる。

(2) P2P技術と分散型合意形成技術

P2P技術は、P2Pネットワークによるデータ通信を可能にすることで、通常のクライアント／サーバ方式のシステムよりもスケーラビリティに優れ、また障害への耐性が強いシステムを実現することができる。これとProof of Workなどの分散型合意形成技術を組み合わせることによって、コンセンサスを得たデータを全てのノードが共有することができ、データの一貫性を保持することが可能になる。

(3) ブリュワーの定理との関係

以上の技術の組み合わせにより、中央管理者を必ずしも想定することなく、データの改竄や二重支払を防ぐとともに、悪意を持つユーザがいても、システムが維持される仕組みを構築することができる、というのがブロックチェーン支持者による主張となる。

なお、分散型コンピュータシステムについてよく知られた定理として、全てのノードにおいて同時に同じデータでなければならないという一貫性、特定のノードの障害によって

他のノードが機能しない状態とならないという可用性、通信障害によるメッセージの損失が起こってもシステムが機能するという分断耐性の3つを同時に満たすシステムは存在しないとされている（ブリュワーの定理）。これとブロックチェーンの関係について見ると、ブロックチェーンは、可用性と分断耐性を備えているが、一貫性についてはどこまで行っても確率的にしか確保されないと評価されることになるだろう。これはブロックチェーンにおけるソフトフォーク現象をとらえたものであり、決済システムへの応用の文脈では、100%のファイナリティは理論的に確保し得ないという主張の根拠となっている(注3)。

(4) スマートコントラクトとの関係

スマートコントラクトとは、契約を表現するメディアを書面ではなく機械とした場合に、書面による契約とは異なる契約制度の実装が必要になるとの仮説のもとで展開される当事者間の私的契約をいう。スマートコントラクトの概念は、ブロックチェーンが開発される以前から存在していたが、ブロックチェーンの登場により大きな注目を浴びることとなったのは、ブロックチェーンがスマートコントラクトを実装するためのテクノロジーの根幹となりうるものであるかとのいうと、現状はまだそれぞれのお考えによるというほかない。ブロックチェーンとスマートコントラクトとの相性の良さが指摘される根拠として、ブロックチェーンがスクリプトによりアプリケーションの実行が可能という特性を持っていることが挙げられる。あとは、利用されるスクリプトがチューリング完全であれば、あらゆるコントラクトを記述することができることになる。ブロックチェーンの中でも、例えばビットコインのスクリプトはチューリング完全ではなく、Ethereum（エセリウム、イーサリアム）のスクリプトはチューリング完全である。

5．ブロックチェーンのビジネス応用

前述のとおり、ブロックチェーンは様々な特性を持つものが開発されているが、いずれも、ビットコイン・ブロックチェーンの実務応用に際しての不都合性や弱点を解決するという思考に基づくものと考えると理解しやすい。

一つには、ビットコイン・ブロックチェーンは、ビットコインという貨幣的価値の移転を表現するものであるところ、これを他の資産の移転や取引の自動執行を実現するといった方向に機能を拡張していくことを指向するサービスが存在する。また、ビットコイン・ブロックチェーンのコンセンサスアルゴリズムを工夫することで、スループットの改善を実現し、より高速な秒間決済を要する取引への応用を指向するサービスも存在する。さらに、前述のとおり、ビットコイン・ブロック

チェーンのパブリック性が取引実務において必ずしも積極に評価されないという実態を踏まえて、ノードの参加者を制限し、より機密性が高く、かつビットコインにおけるProof or Workにまつわる非効率性（決済速度の遅さや全体として見た決済コストの大きさ）に対処しようとする方向を目指すサービスも存在するところである。

それぞれのブロックチェーンは、多くの場合、一定のアプリケーションを見据えてビットコイン・ブロックチェーンの弱みを克服するべく開発されているといえ、改良の方向性を見極めることで、いかなるビジネス用途に応用することができるかが見えてくる。

⑴ ブロックチェーンによって表現する事実関係に着目したビジネス応用

ブロックチェーンは、そのもともとの台帳としての特性から、改竄不能でかつ一貫した資産の帰属履歴を表現するというソリューションを提供するものととらえ、この特徴を活かしたサービスを提供するという方向性の応用がありうる。例えば、不動産や自動車などの権利関係を表示するといったものがありうる。

ブロックチェーンを台帳というスタティックなものとしてとらえる考え方に対して、ブロックへの記述が特定の資産の移転に関するものであることを強調すると、ブロックチェーンは、取引記録を表現するものとしてとらえることもできる。これを押し進めたものがスマートコントラクトの実装としてブロックチェーンを用いるという発想といえる。これは単なる取引記録としての側面を超えて、契約の自動執行という価値をも追求したソリューションとしてブロックチェーンをとらえることにつながっていく。

⑵ 既存の決済システムの置き換え

ブロックチェーンを既存の決済システムを置き換える技術としてとらえた場合、その応用範囲を広げていくためには、ハイ・スループットの実現が重要になる。これを実現するためには、合意形成の方法をより効率化することが必要となり、ビットコイン・ブロックチェーンにおけるProof of Workとは異なるコンセンサスアルゴリズムの採用や、そもそもノード参加者を選別することでシステムの信頼度を高め、コンセンサスアルゴリズムへの依存度を下げる方向性が考えられる。

⑶ 既存のデータベースの補完

ブロックチェーンがP２P技術のもとで分散型合意形成技術を用いることで各ノードが持つ台帳の整合性を維持していることに着目し、分散型リレーショナルデータベースの置き換えとしてブロックチェーンを位置づける例が見られる。これはリレーショナルデータベースがキャパシティを超えたトランザクションに対して脆弱性を持ち、これを克服するための投資額がかさむという現状に対し、ブロックチェーンによる分散処理はキャパシテ

ィを超えたトランザクションに対して自動的な遅延処理を施す仕様となっていることで、より安価に瞬発的な高負荷に耐えられるバックエンドを構築することができるという点を訴求している。既存のデータベースにブロックチェーンをつなぎこみ、ブロックチェーンの特性の一つである分断耐性を利用することで、システム全体の障害への耐性を比較的安価に高めることができるとするものである。

6．終わりに

以上、ブロックチェーンの概要とその構成技術の概説から、これらの技術の組み合わせによって実現するブロックチェーンの技術的な特性を明らかにし、ビットコイン・ブロックチェーンの弱点を踏まえた他のブロックチェーンの改善の方向性と、それぞれのブロックチェーンが目指すアプリケーションないしビジネスについて概説した。

これらのブロックチェーンは、金融（送金、資金決済、証券決済、金融取引）のほか、ポイント、資産管理、登記・登録、認証、物流管理や将来予測、医療情報管理や社内稟議システム、投票その他公共サービスの管理等に用いることができるが、具体的にどの業界に用いることができるかを列挙することは、インターネットをどの業界に用いることができるかを議論するのと同じくらい意味をなさないように思われたため、敢えてそのような個別のユースケースに立ち入ることなく、技術特性から見たビジネス応用の方向性について抽象度を上げた検討を試みた。

ブロックチェーンは、分散化・非中央集権化が進むあらゆる産業セクターにおいて、取引を効率化し、事業のスケーラビリティを高める上で、人工知能と並ぶ革命的な技術となる可能性があると言われている。本稿が、読者諸兄にとって、自らが身を置く業界においてブロックチェーンを具体的にどのように用いることができるかを検討する契機となれば幸いである。

（注１） Bitcoin:A Peer-to-Peer Electronic Cash System（https://bitcoin.org/bitcoin.pdf）

（注２） ビザンチン将軍問題と呼ばれるものである。これは、敵国を取り囲む複数の将軍が、その中に偽の情報を流す裏切り者が存在する状態で、相互に通信し合うことのみによって、戦略の合意形成に至ることが可能かという問題を提示しており、分散システム上におけるノード群のいずれかが偽の情報を伝達する場合に、全体として正しい合意を形成できるかを問うものである。ビットコイン・ブロックチェーンにおいては、Proof of Workにより、悪意のあるノードは、改竄によって利益を得るよりも、マイニングを行ったほうが利益を得ることができるという状態を作り出すことで、このビザンチン将軍問題を解決したものとされている。

（注３） ファイナリティの確保のためにスーパーノードを置くという実装をするブロックチェーンサービスも存在する。この場合、スーパーノードが障害を起こすとブロックチェーンが所期の機能を発揮しないという意味で、可用性を一定程度犠牲にしたものと評価されることになるのであろう。