ブロックチェーン技術が実装されつつある社会

Digital Audit推進部　安達知可良

Chikara Adachi

金融機関等のシステム外部監査や保証業務に従事。金融事業部FinTechセンターのメンバーとして、リサーチ業務のほかFinTech企業等のシステム監査にも従事。また「Digital Audit推進部」を兼務し、ブロックチェーン技術等の社会実装に資する「Digital Trust」の推進を担当。主な著書（共著）に『図解でスッキリ　仮想通貨の会計とブロックチェーンのしくみ』（中央経済社）がある。公認情報システム監査人（CISA）、公認情報セキュリティマネージャー（CISM）、ITコーディネーター。

Ⅰ　ブロックチェーン技術はどういった活用がされているか

1. 注目を集め始めるブロックチェーン技術

暗号資産（仮想通貨）の存在が世間に認知されて久しい中、最近もFacebookを含む団体が独自の暗号資産「Libra」を発行することが発表され話題になっています。この計画が実現すれば、既存の金融サービスを介さない新たな価値交換の仕組みが誕生するかもしれないため、その動向が注目されています。

暗号資産の背景に利用される技術が、ブロックチェーン技術です。ブロックチェーン技術を活用することにより、通貨のようなある種の「価値」を交換する際に、銀行のような「信頼できる第三者」を介さなくとも、その取引の「信頼」が得られるようになるといわれています。第三者を介するビジネスモデルは、こうした「送金」のような領域に限ったものではないので、今、さまざまな業務領域においてブロックチェーン技術の活用可能性の研究が進められています。

2. ブロックチェーン技術の特徴

ここでブロックチェーン技術の特徴を簡単に説明します（＜図1＞参照）。ブロックチェーン技術ではインターネットを介してデータのやりとりが行われます。あるサービスのネットワークがインターネット上に構築され、そのネットワークに参加するコンピューター（ノード）がデータを持ち合う形をとります。従来型システムにて一般的な形態である、1台のサーバー等でデータを一元管理するシステムとはデータの持ち方の点で異なります。

持ち合うデータが正しいものかどうかは、アルゴリズム（いわゆる計算ロジック）により判断されます。各ノードがこのアルゴリズムにより判断を行うことで、いわゆる「衆人環視」の環境を作っているといえます。

このプロセスを経て確定したデータの束（ブロック）が、過去に確定したデータの束と関連付けられるようになっています。この関連付けのための「サイン」のようなものは複雑な計算式により、データの束から自動変換されたものであり、次の世代のデータに関連付けられるようになっています。このため、仮に過去のデータの束が修正された場合、その次の世代のデータにも影響を与える構造になっています。

こうした構造であるため、もしデータを不正に修正することを試みた場合、ネットワーク上に複数存在するノードによる「監視」の目を盗んで、お目当てのデータだけではなく、その次の世代のデータも修正しなくてはなりません。これには複雑な計算が必要となるサインの修正も含まれるため、容易ではありません。このため、ブロックチェーンを使ったシステムは改ざんが難しい点が特徴として認識されています。

Ⅱ　ブロックチェーン技術にはどのような種類があるのか

1. パブリック・ブロックチェーン

ブロックチェーン技術は、代表的な暗号資産であるビットコインのコアテクノロジーとして考え出されたものです。ビットコインに代表されるような仕組みを

▶図1　ブロックチェーンと従来型ネットワークの特徴の比較

	ブロックチェーン（Bitcoin）	従来型ネットワークシステム
ネットワーク構成	▸P2P型 （Peer to Peer） 	▸クライアント／サーバー型 
耐障害性	▸単一障害点がない 一部のノードに障害発生しても、他のノードが稼動していれば情報損失なし	▸単一障害点がある サーバーが単一障害点になるため、バックアップの対応が求められる
改ざん耐性	▸ほぼ不可能 常に他を凌駕（りょうが）する処理能力を持つ環境がない限り、改ざん困難	▸サーバーのセキュリティレベル次第 不正アクセス（内部不正、サイバー攻撃等）のリスクを孕（はら）んでいる
管理者の存在	▸不要 「信頼できる第三者」の存在なく運営が可能	▸必要 中央管理者によるサーバー管理、運用ルールのガバナンスが必要
運営コスト	▸マイニング参加者の自己負担 マイニングのための電力はマイナーの自己負担	▸環境維持のための費用負担 中央管理者に管理費用発生、利用者にコストとして負担させるケースも

「パブリック・ブロックチェーン」といいます。これは、ブロックチェーンのノードとして参加するための制限は特にかけておらず、誰でもブロックチェーン・ネットワークに参加できることから「パブリック」と称されています。

2. パーミッションド・ブロックチェーン

ノードへの参加者を限定している場合を、一般に「パーミッションド・ブロックチェーン」と呼んでいます。文字通り、認められた者のみにノードとしての参加を制限しています。このタイプはさらに、特定の企業等のみにノード参加が許可される「プライベート・ブロックチェーン」と、複数企業から成る団体の参加者であれば参加が許可される「コンソーシアム・ブロックチェーン」に分類することもあります。

いずれのケースにおいてもノード参加者は限定されるため、ブロックチェーン上で発生する取引を確定させる権利や、取引履歴を参照できる権利等が限定されます。こうした特徴を踏まえ、特定の企業間で限定的にデータを共有したい等の場合、このパーミッションド・ブロックチェーンが好まれる傾向にあります。

3. ブロックチェーン技術が活用される領域

こうした特徴のあるブロックチェーン技術を活用した実証実験が、世界中で数多く行われています。B2Bのビジネスモデルの場合、やはりパーミッションド・ブロックチェーン、特にコンソーシアム・ブロックチェーンを採用するケースが多く見受けられます。例えば、貿易金融等、関与者が世界に広く存在し、かつ取引の対象物の状態が適宜変わるビジネスモデルの場合、関与者間で適宜データの更新が行え、すぐに最新のデータを共有することができ、かつデータ改ざんを防止できるブロックチェーンは有用であろうといわれています。

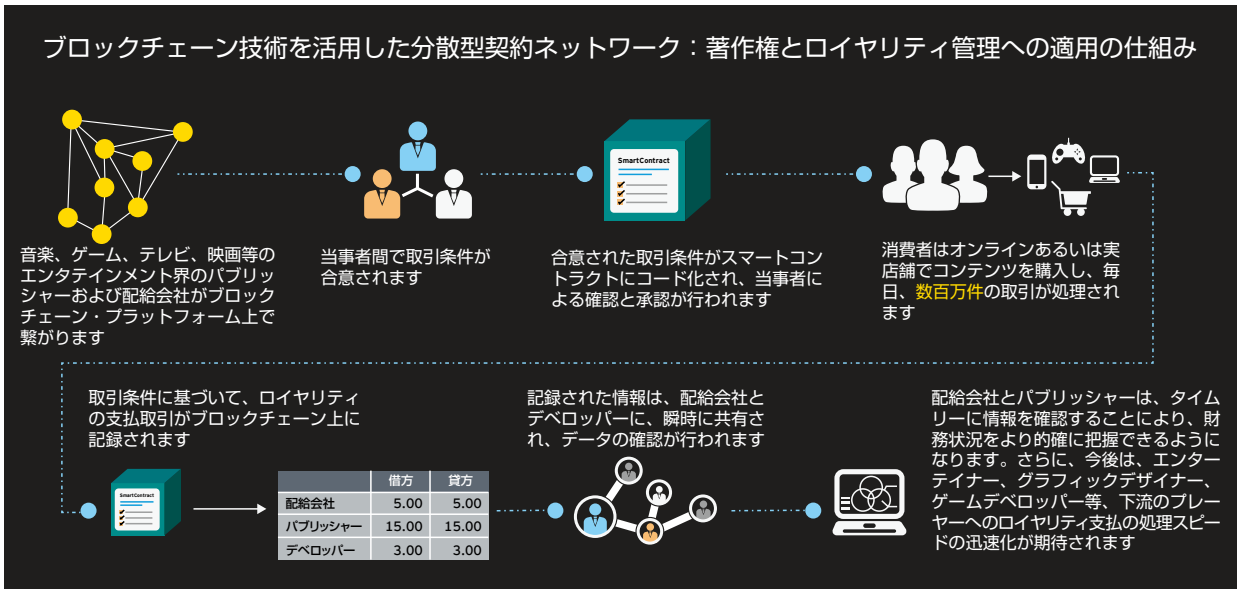
EYもグローバルでブロックチェーン技術を活用したソリューション提供に協力している事例があります。例えば、Microsoft社と協力して、デジタルコンテンツの著作権やロイヤリティの管理システムを合理化するための仕組みをブロックチェーンで開発することを発表しています（次ページ＜図2＞参照）。また、Guardtime社と共同で海上保険における複数企業にまたがるリスク管理のためのブロックチェーンプラットフォーム「Insurwave」を開発しています。

Ⅲ　ブロックチェーン技術が活用されている未来はどうなっているのか

1. スマートコントラクトとしての活用

代表的な暗号資産のプログラムでは、端的に言えば、誰から誰に、いくら送金したかを記録することが行われているわけですが、実はブロックチェーン技術にはさらなる拡張性があります。例えば、なんらかの取引が執行されるための条件をプログラムにあらかじめ設

▶図2　Microsoft社との協業事例



定しておき、その条件を満たした際に、設定されたサービスを自動的に執行させることも可能です。こうした仕組みを「スマートコントラクト」と呼んでいます。

スマートコントラクトを活用すれば、紙の契約を取引の都度締結する必要もなく、またプログラムで決められたサービスのみが提供されることから、効率的、タイムリー、かつ正確な処理が期待できるため、現在注目が集まっています。

なお、スマートコントラクトが、各ノード上で自律的に動くアプリケーション・プログラムである場合、DApps（Decentralized Applications：自律分散型アプリケーション）と呼ばれることがあります。従来型のシステムのようにシステム管理者を明確に特定せず、利用者等により維持・管理されることが特徴です。

また、スマートコントラクトやDAppsの活用がさらに進んで、契約手続から業務の履行、および報酬の支払まで全て自動的に実行されるようになれば、組織運営そのものを自動化できるかもしれません。こうした組織は、DAO（Decentralized Autonomous Organization：自律分散型組織）と呼ばれており、人々の働き方そのものを大きく変える可能性を秘めた仕組みとして注目されています。

2. 社会実装の先にあるもの

ブロックチェーン技術を使ったサービスは、さまざまな実証実験が進められているものの、世に広く利用されるようになるにはもう少し時間がかかると思われます。しかし、いずれは社会インフラとして実装される日が来るとみられています。

ブロックチェーンを活用したシステムの利用が、現在のように一部範囲に限られている場合と異なり、社会インフラとして利用されることになれば、世の中からシステムそのものの信頼性が問われるようになるかもしれません。

例えば、多くのパブリック・ブロックチェーンでは（これ自体が特定の第三者に依存しないブロックチェーンの利点として語られることが多いですが）明確な管理者を設置しないケースも多いことから、実装されているプログラム・ロジックが適切であることの確証がないと利用に不安を感じる場合もあるかもしれません。特にスマートコントラクトの場合、ある条件が満たされれば自動的に後続処理が執行されるようになっているため、プログラム・ロジックに誤りがあると不適切な処理が自動的に執行されてしまうことにもなりかねません。こうした事象を防ぐために、第三者がプログラム・ロジック等を検証するよう求められる時代が訪れることも考えられます。

EYオセアニアでは、AIやRPA等の最新のテクノロジーを活用したビジネスに信頼性を提供する「Digital Trust」というサービスを開始しています。ブロックチェーンについても、スマートコントラクトのレビュー等のサービスメニューを用意しています。