今回の「PwC Technology Forecast」では、ブロックチェーンとスマートコントラクトオートメーションに関するレポート（全5回）とインタビュー記事をご紹介します。

ブロックチェーンテクノロジーについてなじみの薄い方であれば、全5回のレポートを全て読まれることをお勧めします。ブロックチェーンに精通している方は、第1回と第5回だけでも読まれてみてはいかがでしょうか。いずれにせよ、インタビュー記事は一読の価値があります。

第1回　序論と将来像
第2回　ブロックチェーンの定義
第3回　なぜ、ブロックチェーンが重要なのか？
第4回　プライベートブロックチェーンか、パブリックブロックチェーンか、それともその両方か？
第5回　スマートコントラクトがデジタルビジネスをどう自動化するのか？
インタビュー：Coin SciencesのGideon Greenspan氏。パブリックブロックチェーンに代わるものをテーマとしています。

プライベートブロックチェーンが支持される理由

Gideon Greenspan氏
マルチチェーンの開発を手がけるCoin Sciences LtdのCEO

Coin SciencesのGideon Greenspan氏は、パブリックブロックチェーンの法的な問題、企業がパブリックブロックチェーンに代わるものを探し求めている理由について掘り下げます。

インタビュアー：PwCのテクノロジーイノベーションセンター

PwC：ブロックチェーンテクノロジーについての理解という点で、金融機関は、今現在、どのような状況にあるのでしょうか？

GG：金融機関のイノベーショングループ内では、すでに認知度が高くなっています。それ以外のところでも、ビットコインの根幹テクノロジーであるブロックチェーンが、銀行にとっても深い意義を持つ可能性があることを理解する人が増えています。その一方で、このテクノロジーをプロセスの簡略化やコスト節減に活用することが本当に可能なのか、可能であるとしても、どの分野に適用できるのかということに関して、確信できずに戸惑っている様子も少なからず見受けられます。そうした質問に対する包括的な答えをすでに見いだしている銀行は少ないと考えられます。

従って、実際に、ある程度本格的に導入するには2年～3年かかると考えられますが、導入の第一段階はもしかすると相当長期化するかもしれません。ブロックチェーンテクノロジーが現在利用しているテクノロジーをはるかに凌駕するものだとしても、やはり銀行においては、IT、教育研修、組織構造、法規制上の問題点の面で移行コストが大幅にかさみます。その上、何が引き金となってブロックチェーンあるいは他の分散型台帳技術への大規模な移行が起こるかは、まだ明らかではありません。たとえ移行が避けられないとしても、移行するのは容易ではなく、滞りなく自動的に移行が実現するとは期待できないでしょう。

「ブロックチェーンが現実社会で合法的に機能するためには、許可制にしてしっかり管理する必要があるのです。そうでなければ、資産を発行する組織体は違法行為に巻き込まれる危険に身をさらすことになります」

PwC：新たに出現したテクノロジーにより、ある業界の既存事業モデルが破壊される、あるいは効果を失うということがあります。その典型例が音楽業界です。金融セクターのスタートアップ企業はブロックチェーンをどのように利用しようとしているのでしょうか。それによって既存の金融セクターに破壊的インパクトが生じたり、仲介事業が排除されたりするのでしょうか？

GG：現在、世界には、手形交換所、証券保管機関、決済機関、メッセージエンティティなど、金融取引を中央集権的に管理する多数の中央管理機関があります。これらの機関のおかげで、私たちは、金の延べ棒や株券を世界の端から端へ物理的に輸送することなく取引を行うことができます。しかし、これらの機関を脅かすのが単一台帳の力です。台帳は全ての市場参加者間で共有され、その管理も全参加者間に分散されます。要するに、ブロックチェーンは金融仲介機関離れを促すテクノロジーであり、信頼できる取引台帳の維持を主目的とする機関の存在を弱めるものです。

PwC：これらのテクノロジーについて不案内であるため混乱している人も多いようです。ビットコインブロックチェーンと、銀行が関心を寄せているブロックチェーンから着想を得た共有台帳は基本的に何が違うのでしょうか？前者はあくまでも通貨指向で、支払いがP2P（ピア・ツー・ピア）で行われるのに対し、後者は契約や所有権の移転などに重点が置かれています。区別の仕方はこれでよろしいでしょうか？

GG：用語を巡っては多くの議論や混乱が生じています。パブリックブロックチェーンと、プライベートブロックチェーンあるいは共有台帳とを比べることがありますが、この二つは全くの別物です。テクノロジー基盤は共通しているものの、その使用事例や経済的意味では大きく異なっています。これは家庭用コンピューターネットワークとインターネットの違いに多少似ています。両者には技術的に共通点がたくさんありますが、社会的ダイナミクスや目的の面で根本的に異なっています。ビットコインブロックチェーンには非常に興味深いアプリケーションがいくつかありますが、これらのアプリケーションは金融セクターで検討しているプライベートブロックチェーンその他の共有台帳のアプリケーションとは明確に異なります。

例えば、当社はマルチチェーンの開発に取り掛かる前、ビットコイン取引を用いて、ビットコイン以外にもさまざまな資産を移動できるプロトコルを開発しました。なお非暗号通貨資産と言う場合には、必ずある組織体により発行された資産という意味で言っています。さて、このアイデアの問題点の一つとして組織体がビットコインプロトコル上で移動可能な資産を発行した場合、その資産が全くの無記名証券となることがあげられます。無記名株式や無記名債券がほとんど使用されなくなっているのには理由があります。不正目的で利用される恐れがあるからです。

このため、資産を取引できる者に関する制限が一切ないパブリックブロックチェーン上で資産を発行するというアイデアに真面目な企業が乗ってくるはずがない、という結論に達しました。それがパブリックブロックチェーンとプライベートブロックチェーンが全くの別物であるというもう一つの理由です。ブロックチェーンが現実社会で合法的に機能するためには、許可制にしてしっかり管理する必要があるのです。そうでなければ、資産を発行する組織体は違法行為に巻き込まれる危険に身をさらすことになります。

「プライベートブロックチェーンに対して、過剰な期待を膨らませている人もいるようですが、プライベートブロックチェーンの登場によって、取引される資産の法的性格が変わることはありません」

PwC：単なる分散型データベースではなく、プライベートブロックチェーンが利用される主な理由は何ですか？

GG：プライベートブロックチェーンに対して、過剰な期待を膨らませている人もいるようですが、プライベートブロックチェーンの登場によって、取引される資産の法的性格が変わることはありません。少なくとも当面の間は。プライベートブロックチェーンがどのようなものであるかと言うと、誰が取引資産を所有しているかを把握する上で、共有台帳を極めて効率的に管理するテクノロジーです。別の言い方をすれば、ブロックチェーンとは、必ずしも絶対的と言える信頼がない環境においても、データベースの共有を可能にする、しかもそのデータベースを管理するためのゲートキーパーの存在が不要なテクノロジーだということです。既存の分散型データベースと比べると、プライベートブロックチェーンは革新的な特性を数多く備えているので、金融機関間のP2P金融取引に適しているのです。

ブロックチェーンの一部の側面には、既存のデータベーステクノロジーが踏襲されています。一例として「多版型同時実行制御」（MVCC）というテクノロジーがあります。MVCCはトランザクション同士が衝突したり速度を低下させたりすることなく、複数のトランザクションが単一のデータベースに同時にアクセスすることを可能にするためによく用いられている方法です。ビットコインの創造者たちは、そうとは知らずに、これと同じ技術を作っています。ただし中央管理される単一のデータベース内ではなく、分散的な方法でネットワーク上に同じ機能を実現したのです。

ブロックチェーンには、今日の分散型データベースにおいて提供されていない重要な特性がさらに二つあります。第一の特性が、取引レベルの制約です。つまり個々の取引について、その取引全体を検証することで確認するということです。今現在、データベース内の許可システムは、誰が特定のテーブルを修正する許可を有しているかを管理し、それらのテーブルに含めることができる情報を制約しています。しかしながら、そこには、「条件X、Y、Zを満たしている取引のみが有効である」というようなルールが設けられているわけではありません。ブロックチェーンは、このようなルールに基づいて、取引の有効性を検証するケイパビリティを備えています。これは、信頼関係にない組織体の間でデータベースを共有する場合には極めて重要です。

第二の特性が、公開鍵暗号の使用です。これにより、中央管理者による検証がなくても行レベルの許可を与えることが可能になります。従って、一つ一つの取引にその取引によって変更される行の所有者が取引を承認したというプルーフが含まれることになります。また、このプルーフは、ブロックチェーンネットワークの全参加者によって確認されます。

PwC:ということは、ビジネスプロセスにおいて暗号通貨が不要である場合、もしかすると最終的にはもっと高度なデータベースの一部となる可能性がある特性を利用することになる、ということですね?

GG: そのとおりです。私は、ブロックチェーンがセキュリティ管理やP2Pにおいて複製シナリオの同期を取る新たな方法として、最終的に既存のデータベースプラットフォームに統合される可能性があると考えています。ただし具体的なユースケース向けにこのテクノロジーを応用することで、新しい製品が登場してくる可能性も多分にあると期待しています。

お問い合わせ先

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200(代表)

松崎 真樹	*田中 玲*	*一山 正行*
パートナー	パートナー	ディレクター
maki.matsuzaki@pwc.com	rei.r.tanaka@pwc.com	masayuki.m.ichiyama@pwc.com

「PwC Technology Forecast」について

PwCのテクノロジーイノベーションセンター(CTI)が刊行する「Technology Forecast」は、新たなテクノロジーや最新動向について掘り下げ、経営者やテクノロジー担当幹部の皆様をテクノロジーがもたらす機会における活用戦略の開発面で支援いたします。

これまでの「PwC Technology Forecast」では、さまざまな新テクノロジーやトピックを取り上げてきましたが、その多くが、今日のテクノロジーやビジネスに係る主要問題となっています。「Technology Forecast」についての詳細は、www.pwc.com/technologyforecastをご覧ください。

www.pwc.com/jp

本報告書は、PwCメンバーファームが2016年5月に発行した『The argument for private blockchains』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル(英語版)はこちらからダウンロードできます。 www.pwc.com/us/en/technology-forecast/blockchain/gideon-greenspan-interview.html
日本語版発刊月: 2016年9月　　管理番号: I201605-12