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：ブロックチェーンの定義

第2回（全5回）

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最終的に実現するのは、デジタル通貨以上のもの、すなわち、デジタル・ビジネス・フローである。

pwc

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。

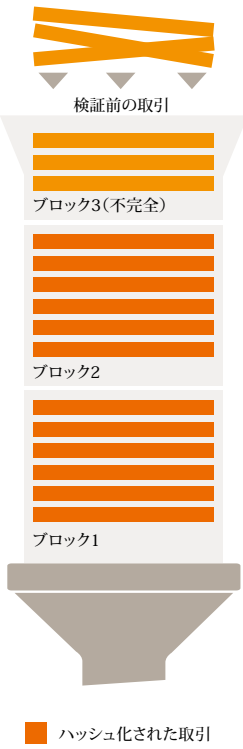
第1回　序論と将来像
第2回　ブロックチェーンの定義
第3回　なぜ、ブロックチェーンが重要なのか？
第4回　プライベートブロックチェーンか、パブリックブロックチェーンか、それともその両方か？
第5回　スマートコントラクトがデジタルビジネスをどう自動化するのか？
インタビュー：Coin SciencesのGideon Greenspan氏。パブリックブロックチェーンに代わるものをテーマとしています。

ブロックチェーンの定義および定義の変化

ブロックチェーンはスマートコントラクトを実現する中核的技術である。本セクションでは、一般的なブロックチェーンと銀行業界特有のブロックチェーンとを比較・対比し、銀行業界から見たブロックチェーンテクノロジーについて述べていく。

ブロックチェーンはビットコインなどの暗号通貨の基盤となるテクノロジーであり、一言で言えば、共有デジタル台帳、すなわち継続的に更新され続ける全取引のリストである。この台帳は中央管理されず、完全な分散型P2P（ピア・ツー・ピア）ネットワーク上で生じる全ての取引を一つ一つ記録していく（ネットワークはパブリックである場合も、プライベートである場合もある）。ブロックチェーンの信頼性は、既存の取引記録（ブロック）を認証し、連鎖させる強力な暗号にかかっており、この暗号によって検知されることなく、個々の取引記録を改ざんすることがほぼ不可能となる。

ブロックチェーンとは何か？



ブロックチェーンとは、中央管理されない分散型の取引台帳であり、この台帳はネットワーク中の各ノードで保存されており、共有の台帳として、各ノードにより所有、維持されるとともに同期して更新され続ける。P2Pシステムであり、取引フローを管理する中央管理機関は存在しない

ブロックチェーンというネーミングは、ハッシュ化された取引が変更不可能な形で順番に台帳に追加される様子の***視覚的な描写***に由来する

ハッシュとは、取引データの秘密を保持するために、実際の取引データが暗号化ツールを経由したときに生成される、独自の識別子およびショートカットである

ビットコインブロックチェーンなど、ブロックチェーンの最も有用な要素の中には次のようなものがある。

1. デジタル署名：
   a. 秘密鍵所有の検証
   b. メッセージが正当な相手から発信されたかどうかを検証
   c. メッセージが改変あるいは改ざんされていないかどうかを検証
   d. 文書や契約書のきめ細かなバージョン管理が可能
2. 電子署名が付される取引ブロック：
   a. 取引シーケンスを保護
   b. 個々の取引レベルできめ細かなアクセスコントロールが可能
   c. 監査証跡を継続的に更新・作成
3. 分散型共有台帳：
   a. 真実の取引記録を唯一のバージョンとして確定
   b. 第三者が中央管理を行う必要性を低減あるいは解消
   c. スマートコントラクトテクノロジーを前提として成立する自律的なエージェント、プロセス、組織に門戸を開放

暗号通貨にも独自の強みや有用性があるのは言うまでもない。とりわけビットコインなどデジタル通貨を伴う取引は、スマートコントラクトケイパビリティの中核となり得る。最も分かりやすいケースでは、スマートコントラクトにより、レンタカー運転契約期間が切れたドライバーを締め出すことが可能になる。より複雑なシナリオでは、レンタカー会社が施設全体の業務を自動化することも考えられる[1]。

ブロックチェーンの定義にはさまざまな解釈の余地がある。場合によっては、暗号通貨の役割を解消あるいは縮小し、プロセス改善を目的として、ブロックチェーンを自ら利用することに焦点を当てているものがある。例えばEris Industriesなどのスマートコントラクトベンダーは、通貨の問題にそれほど深くかかわろうとはしていない。Eris IndustriesのCEOであるCasey Kuhlman氏は、「企業という文脈での真の課題は、所有権移転を単に表現すること（貨幣の役割）ではなく、変わる可能性がある所有権に係るプロセス全般にあるのです」と述べている。その典型例が、証券の組成やトレーディングである。

銀行業界では必要に迫られてブロックチェーンに関し業界なりの定義を作り上げてきたが、それは一般企業にもおおむね適した定義と言える。さらに銀行業界によるブロックチェーンの定義は、暗号化され、変更不可能な共有取引台帳を実現している中核的ブロックチェーンテクノロジーを用いて、銀行が何をしようとしているのか、彼らの意図を雄弁に物語っている。銀行業界の描く長期計画においては、スマートコントラクトがブロックチェーンの最重要用途となる。スマートコントラクトとは共有台帳に格納されるコンピューター処理が可能な契約であり、取引のプロセスにおける人間による検証の必要性を劇的に減らすことができる。

---

[1] スマートコントラクトテクノロジーの法的側面に関しては、Samuel Bourque and Sara Fung Ling Tsui, "A lawyer's introduction to smart contracts"を参照。http://www.crypto-law.com/doc/A%20Lawyer's%20Introduction%20to%20Smart%20Contracts.pdf, 2014（参照日:2016年2月11日）さまざまな複雑さの自律的な分散型ビジネス活動の概念化に関しては、"A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum white paper（2015年11月15日）を参照。https://github.com/ethereum/wiki/wiki/White-Paper（参照日:2016年2月11日）

2015年9月ロンドンで開催されたフィンテックウィークで、聴衆の一人が「企業向けブロックチェーン」のパネリストに対し、「ブロックチェーンを1、2行で簡潔に定義していただけますか」と尋ねたところ、バークレイズのCTOオフィスに所属するパネリストLee Braine博士（コンピューターサイエンス）が次のように答えた。「取引をブロックと呼ばれるバッチにまとめて、次に、直前のブロックにつなげてハッシュ化することにより変更できなくする方法です」

（ハッシュとは固有のデジタル指紋のようなものである。ファイルを固定長ビット列で表したものであり、この利用によって改ざんを防ぐ。さらに直前のブロックとつなげてハッシュ化する（このようにブロックをつなげていくからブロックチェーンと呼ばれる）ことで、チェーンのどの部分も改ざんが一層困難になる。

R3（ブロックチェーンの標準規格策定を目指す銀行から成るコンソーシアムが出資した民間会社）のテクノロジー部門長であるパネリストRichard Brown氏が、上記の定義に少々付け加えた。Brown氏によると、ブロックチェーンという用語は、ビットコインで用いられる、匿名の公開・共有台帳だけを指すものではない。ビットコインブロックチェーンの構造を分解し、そこから有用な部分を取り出して「新しいものを作り出すための構成要素」として用いることができる。従って「ビットコインの問題について述べる必要はない」とのことだ。

両氏の定義は銀行業界の考えをおおむね正確に反映したものと言える。銀行はブロックチェーン現象というこの新しい現象を、必ずしもデジタル通貨と結びついたものとしては見ていない。むしろビジネスプロセスをリエンジニアリングする触媒として、未だかつてないプロセス効率化の好機を見ている。彼らの眼から見れば、マスコミを賑わせているビットコインを巡る話題の大半は的外れなものであるか、少なくとも大手金融機関が期待している潜在的利益の全体像をとらえたものではない。ブロックチェーンテクノロジーの仕組み自体が金融機関の管理プロセスの非効率を永久に追放する方法を指し示しているのである。各金融機関がコストの上昇、規制当局による厳しい監視、競争の激化に悩まされているこの時期、これ以上ない絶好のタイミングで好機が到来しているのである。

次回：なぜ、ブロックチェーンが重要なのか？

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『Blockchain and smart contract automation: Blockchains defined』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/definition.html
日本語版発刊月： 2016年9月　　管理番号： I201605-8