

講演抄録

FinTech におけるブロックチェーンの将来と課題

株式会社 NTT データ
金融事業推進部 技術戦略推進部
システム企画担当部長

赤羽 喜治

1. はじめに

FinTech とは金融を意味する Finance と技術を意味する Technology を組み合わせた造語で、「情報技術を活用して金融サービスを生み出す動き」のことをいう。

従来型の金融機関は、全てを自前で維持改修しデータも整備するモノリシック（1枚岩）なシステムである。一方、急速に拡大している FinTech 時代の金融機関は、様々な外部の金融機関あるいは金融機関ではない企業と緩やかに連携するエコシステムのものへと変化することで、環境変化への即応性を向上していくシステムである（図1）。

FinTech には、既存技術により新規サービスを創出する「オープン API」技術と、新技術により新規サービスを創出する「ブロックチェーン」技術という2つの方向性がある。特にブロックチェーンは、分散型で信頼できる“状態”を創る／維持することを可能にする新しい技術で、現在注目を集めている。この方向性の一例が、2016年7月に発表された「銀行基幹系システムをブロックチェーンで置き換えることを目指す Vault OS」プロジェクトである。

同プロジェクトは銀行基幹システムをクラウド上で提供し、基幹業務を保有せず、データ共有やシステム関連系をブロックチェーン上で行うという、最も極端であるが世の中の方向性を象徴する事例である。

本稿では、新技術ブロックチェーンの将来と課題を考察し、NTT データが考えるブロックチェーンの可能性を紹介する。

2. ブロックチェーンとは

ブロックチェーンは、2008年～2014年頃にビットコイン（仮想通貨）を実現する技術として誕生した。その後、2015年頃～現在は仮想通貨領域以外、例えば貿易金融領域や証券・製造領域など汎用的な分散基盤として拡大し、“ビットコインのブロックチェーン”から“ブロックチェーンが実現する分散型台帳”となった。これまで各システムが個別にデータベースに格納していた台帳データがブロックチェーン技術によってネットワークを介して共有できるようになった。つまりデータを保有する形のパラダイム変化である。

(1) ブロックチェーンの基本的な仕組み

ブロックチェーンの仕組みを簡単に説明する

従来モノリシックだった金融機関のシステムはFinTechの時代には「サービスを外部に提供し、また外部から取り込む」「データも外部連携し、共有する」ことを通じて、エコシステム的なシステムへと変化し、環境変化への即応性を向上させていくと考えられます。

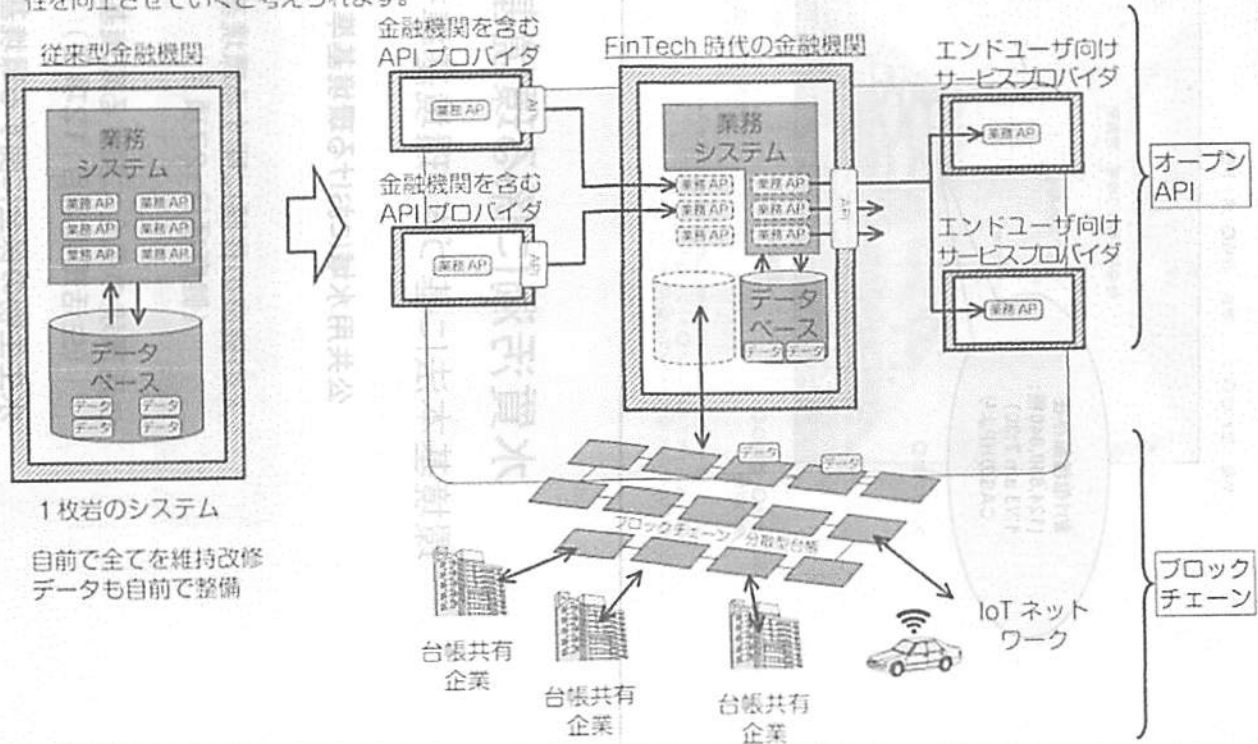


図1 FinTech時代の金融機関システム

と、取引内容等をまとめたブロックをつなげたものである(図2)。ネットワーク上で互いにデータを持ち合い、全員が検証可能とすることで信頼できる状態を作り、維持する仕組みである。

(2) 分散型台帳とは

分散型台帳を説明するには、データベースサーバと対比するとわかりやすいと思われる。

「データベースサーバ」は、複数のユーザから同じデータに対して書き込み要求がある時、1つの要求は受け付けて、その間の別の要求は抑止する、アクセスコントロールを行っている。一方、ブロックチェーンが実現する「分散型台帳」は、同じ台帳データが複数のシステムに配置されて同期をとっており、複数のユーザから同じデータに対して書き込み要求がある時、各システム間での合意形成ルールに基づいてどの書き込みを同期するか皆で決める、コン

センサスアルゴリズムを行っている。つまり、参加している全システムがそれぞれ台帳データを保有し、常に同期をとるというデータの持ち方が分散型台帳であり、これを実現するための状態の共有や合意形成の仕組みの1つがブロックチェーン技術である。

各システムからはブロックチェーンの中で起こっていることは見えず、あたかも1つの台帳に対して各システムがアクセスしているように扱われる。分散型台帳は、例えば貿易業務、サプライチェーン(原材料・部品、製造、在庫管理、販売、配送までの製品の全体的な流れ)、トレーサビリティ(生産段階から最終消費段階まで追跡可能な仕組み)などの複数の組織が連携する領域において真価を発揮すると考えている。例えば輸出者が書き込んだ輸出品の情報を、輸入者は容易に見ることができることで何

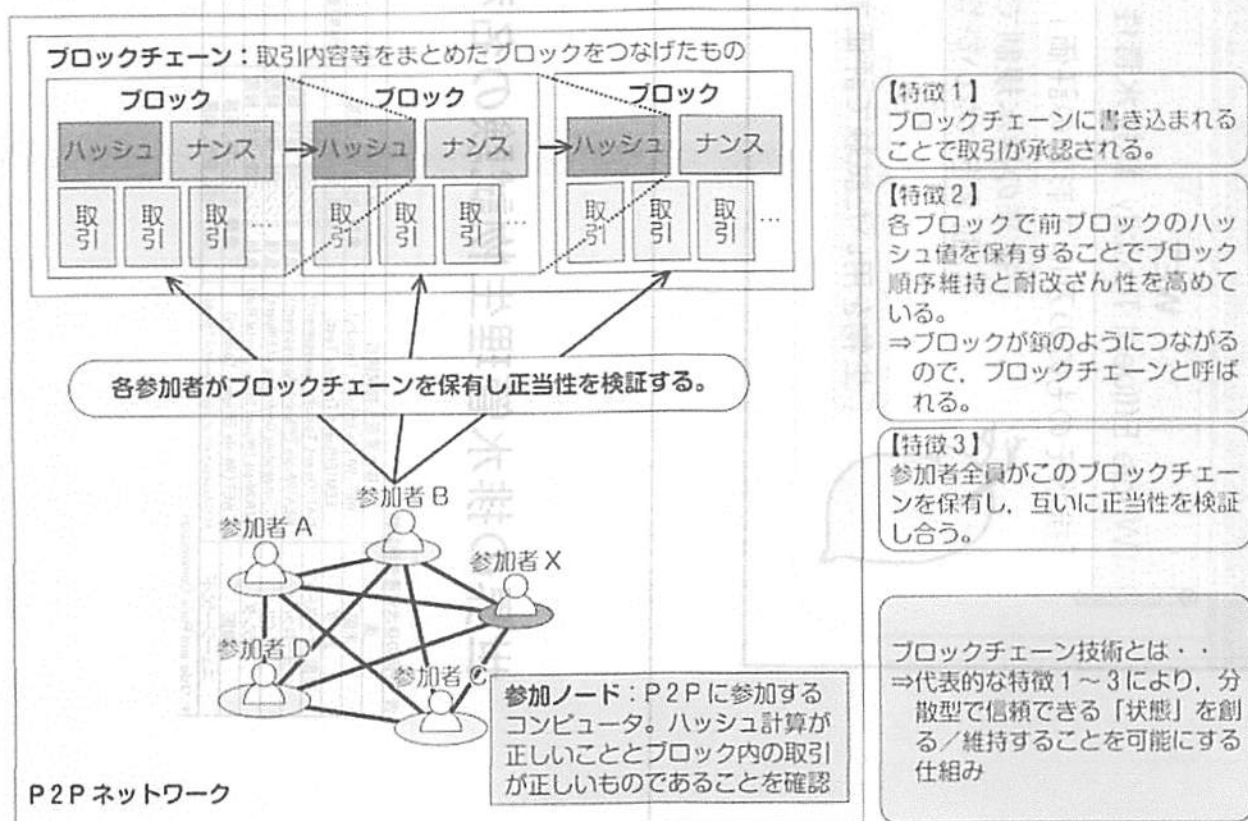


図2 ブロックチェーンの基本的な仕組み

かあった時にすぐに対処ができる。金融分野ではリファレンスデータ（銘柄情報や顧客情報）管理にも活用できる。

(3) ブロックチェーン技術の特長

ここまでのブロックチェーンの特長をまとめると、①データの透明性・トレーサビリティが可能、②関係者間の直接的な情報の共有・管理（皆が同じデータを持っているため改ざんができないということにつながっていく）、③改ざんが困難な仕組み／記録の不可逆性（誰がいつ何を操作したか全て記録が取られる）、があげられる。

3. ブロックチェーン技術の応用例

(1) 電力市場への応用

電力市場におけるブロックチェーン技術の応

用例は、TransActive Grid 社が「TransActive Grid プロジェクト」という、自家発電で余った電力の直接的な取引を可能にする実証実験がある。ソーラーパネルなど発電機をもつ家庭が余剰電力の取引をする時、従来は電力会社の仲介が必要だが、ブロックチェーンを活用することで仲介不要で直接取引が可能となった。これにより供給者・受給者双方に大きな経済メリットを享受できるようになる。

(2) 著作権管理への応用

著作権管理についても、従来はデジタルコンテンツに電子透かしのようなものを登録して違法アップロードを検出する第三者機関の証明が必要であった。しかしブロックチェーンを活用すると、改ざん耐性を備えた著作権情報をオープン化して共有することで著作権証明が可能となり、第三者機関が不要となる。すでに

Blockai社はブロックチェーンを活用した著作権証明サービスを提供している。

(3) 高額商品のトラッキングへの応用

Everledger社のダイヤモンド取引管理サービスは、ブロックチェーンの応用によくあげられる例である。ダイヤの所有者・保険・鑑定件などの情報をブロックチェーンで管理するサービスで、ブロックチェーン上に売買の記録、ダイヤの特徴や画像を記録し、全ての取扱業者が見えるようにすることで、自分のところに届いたダイヤは異常な状態で取引されていないか検知できるようになる仕組みである。

(4) IoTビジネスへの応用

IoTビジネスには、ブロックチェーンを活用した方が効率の良い分野がある。その一つの例にSlock社が行っている、様々なモノを「借りる・売る・シェアする」仕組みをブロックチェーンで実現する実証実験がある。従来は物の貸し借りにおいて人が介在する必要があったが、IoTとブロックチェーンを組み合わせることで人が介在しない貸し借りサービスが可能になっている。

(5) 政府の応用例

① エストニア政府の取組み

エストニア政府はITの導入に非常に先進的な取組みを行っており、ブロックチェーンを、医療データの記録（国民の健康医療データをブロックチェーン上に記録する実証実験を行い個人情報保護しつつ有用な医療情報の流通を可能にするサービス）と、公証サービス(e-ResidencyというIDカードを発行してもらうと、国境を越えた婚姻証明や出生証明、事業契約が可能となり、エストニア国内で企業を起こすこともできる資格サービス)に活用している。

② 日本の経済産業省の取組み

日本では、経済産業省が「ブロックチェーン

技術を利用したサービスに関する国内外動向調査」を2016年4月に公表した。それによると、ブロックチェーンを活用した新ビジネスの検証のための民間実証の促進と成果および課題の集積を行い広く公開していくことで市場の発展を促すこと、ブロックチェーンの社会実装を円滑に行うため必要に応じて規制等を見直すこと、などとまとめている。

(6) ブロックチェーンの特性とは

ブロックチェーンの利点は次の4点である。

- ①データの高い透明性・トレーサビリティ、②仲介者を介さない直接的なやり取り、③高改ざん耐性、④単一障害点がない（高可用性）。

一方で、課題も次の3点がある。①P2Pネットワーク上で動作するための遅延、②高可用性だけが重視されておりデータの一貫性や分断耐性が不十分（CAP定理）、③方式によってはデータのファイナライズが不確定。

これらのことから、ブロックチェーンとの相性の良い領域、つまり「台帳を共有することで価値を見出せる領域」と「リアルタイム性を求められない領域」での導入に向いていると考えられる。

4. ブロックチェーンの論点

(1) The DAO Attack 問題

2016年6月に「The DAO アタック問題」が発生した。The DAOとはドイツのスタートアップ企業Slock.it社がはじめたクラウドファンディングサービスで、スマートコントラクトを使って作られた資金を集めるプログラムをDAOとよぶ。自律分散型の投資ファンドとして注目され、1カ月で150億円集めるなど画期的なスタートを切った。そのDAOプログラムの脆弱性について、50億円が引き出されかかっ

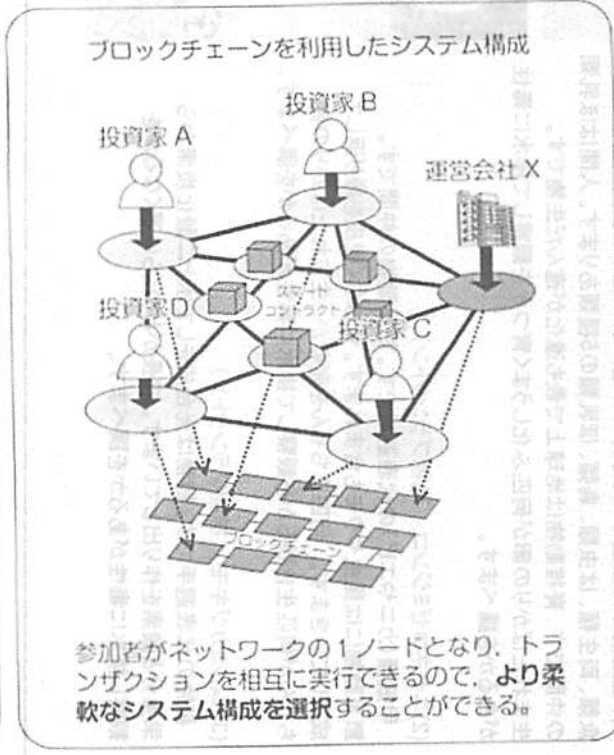
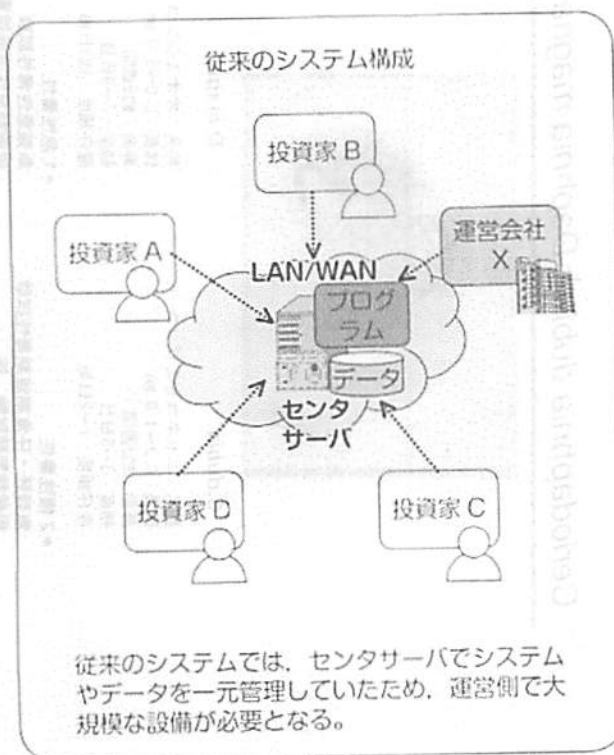


図3 従来システム構成との比較

た（引き出される前に以下の対処をしたので、未遂に終わった）。

事件としてはハッキング行為であるが、問題は犯罪者が行った送金記録が、対改ざん性が売りのブロックチェーンに書き込まれてしまったことである。同事件の対処は、犯罪者が書き込んだブロックは読み込まないことにし、50億円はコントロール下にある別のファンドに振り込まれたことにしてそこから被害者に返金するという、過去を書き換えることを行ったのである。

(2) Ethereum ハードフォーク問題

ブロックチェーンを不正が行われる以前に巻戻す（ハードフォーク）という新たな可能性を自ら作り出してしまった。これは、ブロックチェーンを信じていた人にとって大変な反発を呼び、ブロックチェーンの存在意義自体に関わる問題と議論が続いている。本件で垣間見えたように、何らかの原因で正しくない情報がブロックチェーンに書き込まれてしまった場合の

運用対処方法は重要な視点となる。

ブロックチェーンを構成する各技術のレイヤーごとに技術の深堀と検証が必要で、メンバーシップ管理など従来システムと同様の安全対策が求められるレイヤーと、ブロックチェーンならではの視点が求められるレイヤーとがあり、特に後者についての蓄積が求められている。

5. NTT データの取組み例

NTT データはブロックチェーンをどのように進めていくのか紹介する（図3）。NTT データのブロックチェーンを利用したシステムは、データをブロックチェーン上に分散台帳という形で保管し、ブロックチェーンを構成するノード上で処理結果をブロックチェーンに書き込むスマートコントラクトというプログラムで構成される。このような柔軟なシステム構成は今ま

個の影響力拡大が社会の変革を促進する

オープンな連携が新たな社会の仕組みを生み出す

進化する価値が規制概念の転換を促す

フィジカルとデジタルの融合が持続性と迅速性をもたらす

- こうした社会変革で求められる、新しい社会インフラに必要な技術の一つ
- 現在の情報システム体系において、重要となるネットワークコストとセキュリティを同時に実現できる点において優れている
- 金融分野に限ったことではなく、社会全体に適用可能性があると考えている

だからこそ、NTTデータが取り組む必要がある

図4 NTTデータにとってブロックチェーンとは何か

ではかなり異なるため、多くの実証実験を行い、NTTデータとしてノウハウを貯めていく必要がある。

6. データ共有・サービス共有の先にあるもの

中心が存在しない分散型の組織・情報伝達が浸透すると、全てが分散前提となる。ただし、分散していくと何が起きるかという、意図しない情報流出が問題となる。ブロックチェーンは全ての人と同じ情報を持つことがメリットであるが、逆に言えば情報と関係のない人にまで見られてしまうことがある。そこで情報保護の技術もセットにして講らなければならない。

NTTデータはNTT持株研究所と連携して、アクセスコントロールや情報保護機能を開発し

ており、2016年12月から実証実験を行っている。情報保護の技術があって、初めてブロックチェーンにおける分散型台帳が意味のあるサービスとなる。

7. おわりに (図4)

(1) NTTデータの考えるブロックチェーンとは

ブロックチェーンは新しい技術であるが、新しい技術によって可能性が広がっていくというのは、今までの歴史の中で繰り返されてきたことである。それと同時にメインフレーム（既存型）が全てなくなることはなく、分権型システムは中央集権型システムを全て置き換えるものではない。例えば、LinuxやUnixのような

オープン環境やクラウドコンピューティング技術は、消費者の選択肢を広げつつ一部を置き換える技術となっている。ブロックチェーンも複雑で費用対効果が見込めなかった領域をシステム化できるようにする技術であり、事業スコープを周辺に広く拡大させる可能性を持つものである。

(2) NTT データにとってブロックチェーンとは何か

NTT データの今後の戦略は、①実証実験による技術蓄積と補完、②分散型台帳としての拡がりの追求、③新しい社会インフラの構築、の

3点について取り組んでいく。

ブロックチェーンの意義は、会社と会社、あるいは業界と業界、国と国、といった横串を通して情報連携していくということである。それを突き詰めていくと新しい社会インフラに近づいていくといえる。また、金融分野だけではなく、社会全体の複雑な領域に適用の可能性があると考える。NTT データは、これまで担ってきた金融システムやクレジットカード決済ネットワークシステムの知見があるからこそ、ブロックチェーン技術に取り組む必要があると考えている。

本稿は一般社団法人電気通信協会産業部会が平成29年1月31日に開催した第134回ブロードバンド・ユビキタス調査会における講演から抜粋してとりまとめたものです。

ISSN0911-7601

昭和26年10月19日第3種郵便物認可
2017年5月1日 毎月1回1日発行

電気通信

Vol.80 No.844

2017-5

電気通信事業分野の政策動向

巻口 英司

電気通信 5月号 Vol. 80 No. 844
2017年5月1日 発行
定価 810円(本体750円)

発行人 祖父江和夫
発行 一般社団法人 電気通信協会
〒101-0003 東京都千代田区一ツ橋二丁目1番1号
如水会ビルディング6階
電話 (03)3288-0604 FAX (03)3288-0615
ホームページアドレス <http://www.fta.or.jp/>
振替口座 00190-2-2884番

無断転載禁ず

法人会員・個人会員関係のお問い合わせ：業務部 (03)3288-0605
産業部会会員関係のお問い合わせ：産業部会 (03)3288-0603