

ブロックチェーンの特性から理解する社会実装の展望 効率化・コスト削減から高付加価値創出へ

ブロックチェーンはビジネスにおいて戦略的に重要な技術として選ばれ始めている。ブロックチェーンは中央管理者無しに信頼性の高い記録によって取引を成立させることができる特性を持っており、これによって契約やワークフローの効率化・コスト削減効果が期待できる。そして、普及の段階を経て、例えば競争領域での競合他社間の協調のような新たなデータ共有の形といった高付加価値を創出していく。

1. グローバルにおけるブロックチェーンの潮流

金融以外の産業でもブロックチェーンはビジネスにおいて戦略的に重要な技術として選ばれ始めている。デロイト トーマツが世界 12 カ国のシニアエグゼクティブ 1,386 名を対象に実施した「デロイト グローバルブロックチェーンサーベイ 2019」¹では、調査対象の半数がブロックチェーンに対して「戦略プライオリティのトップ5に入る」と回答しており、経営戦略上重大であるとの認識は 8 割を占めた (図 1 参照)。この調査の回答者は通信や製造の業種からも構成されている (図 2 参照)。

図 1 ブロックチェーンの関連度に対する見解

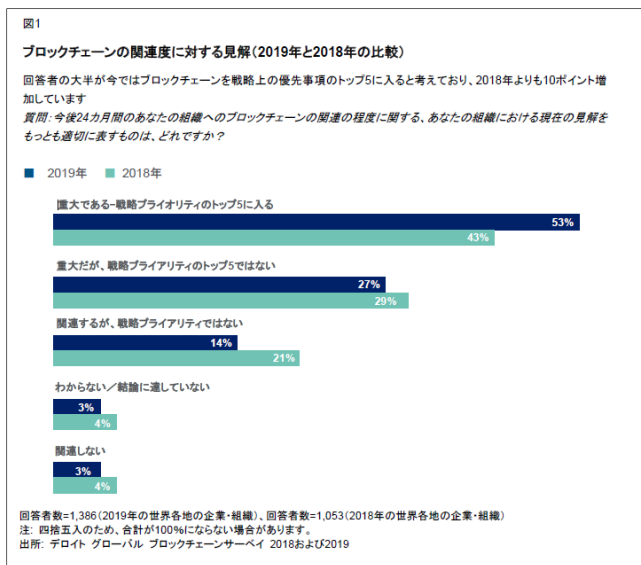
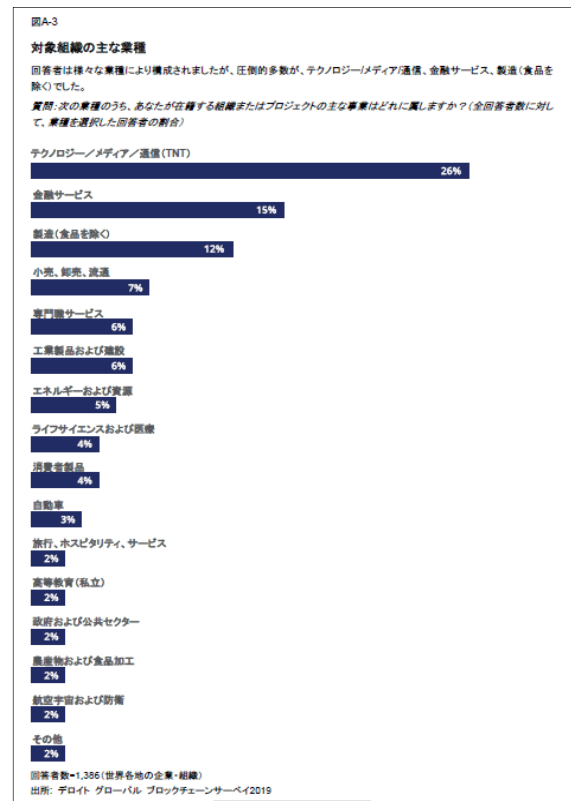


図 2 対象組織の主な業種



デロイト トーマツ グループ「デロイト グローバル ブロックチェーンサーベイ 2019」より出典

ブロックチェーンは各国政府の取り組みにおいても重要視されている。暗号資産の取引に対して厳しい規制を敷い

¹ <https://www2.deloitte.com/jp/ja/pages/risk/articles/ra/global-blockchain-survey-2019.html>

ている米国と中国はブロックチェーンという技術自体へは肯定的な姿勢で、金融以外の分野への導入を進めている。

米国の疾病対策センター（CDC）では健康や衛生へのより深い洞察を得るために電子健康記録（EHR）を収集する台帳をブロックチェーン技術によって作成する取り組みがなされている²。また、技術的な取り組みに留まらず、バーモント州はブロックチェーンに記録された土地登記記録が法的に有効であると認めるための法整備も同時に進めている。

中国は国家におけるイノベーション戦略の一つとしてブロックチェーンを重要視しており、「第 13 次五ヶ年計画」に AI、IoT、クラウド、ビッグデータやバイオテクノロジーと同列に「区块链（ブロックチェーン）」を並べている。

2. ブロックチェーンの特性

ブロックチェーンが従来のシステムと違ってユニークであるポイントは、中央管理者無しに信頼性の高い記録によって取引を成立させるところにある。特定の管理者が見張らずともブロックチェーン上の記録に対しては改ざんや二重取引ができないようになっており、安心して価値あるものの取引をブロックチェーン上に委ねることができている。改ざん耐性をどのように維持しているかという点、ブロックチェーンシステムの利用者たちで集まってネットワークを作り、この利用者たちがそれぞれ個別に記録台帳の全件を保持することで成立させている。例えば、暗号資産 Bitcoin の場合は全送金記録を全ての Bitcoin の利用者たち、いわゆるノードが保持している。記録台帳を改ざんしようとしても、少なくともこれらの半数以上を対象に改ざんしなくてはならない。

ブロックチェーンによる価値交換を成立させている特性を以下に挙げる。

(1) 分散型台帳

記録台帳の全件を保持する個々のノードはネットワーク上に分散しており、その台帳は分散型台帳と呼ばれる。あるノードで更新があった場合も常に全ノードで同期がとられ、各ノードが常に同じ台帳データを保有できるように維持されている。そして中央管理者がいない代わりにネットワーク参加者全員で共有・検証・更新を行い、台帳記録の信頼性を保っている。

ブロックチェーンプラットフォームによっては例外があるものの、基本的には全てのノードが同じ台帳データを保有しているため、データを独占したり規制をかけたりするような権力者がおらず、どのノードも平等な立場にある。この分散型台帳の特性によって、企業間の P2P 取引や承認プロセスを効率化することができるようになる。

(2) コンセンサスアルゴリズム

コンセンサスアルゴリズムとは、分散台帳に更新があったときにどのように更新を承認していくのかを取り決めたルールである。ブロックチェーンは取引や更新の記録（トランザクション情報）、記録日時（タイムスタンプ情報）、そして一つ前のブロックのデータのハッシュ値³などを「ブロック」と呼ばれる一つの形にまとめている。この「ブロック」がハッシュ値によって古いブロックから新しいブロックへと順に鎖のように繋がっていくので、「ブロックチェーン」と呼ばれている。また、連なりの次のブロックを生成することを更新の承認と呼ぶが、承認ルールにはいくつかの異なる形式がある。

² <https://www.ibm.com/case-studies/centers-for-disease-control-and-prevention>

³ ハッシュ値とは元になるデータから計算により求められる不規則な値。元となるデータに 1bit でも差があれば、計算の答えとなるハッシュ値はそれぞれ違った値となる。

Bitcoin と Ethereum⁴は PoW(Proof of Work)と呼ばれるコンセンサスアルゴリズムを採用している。PoW においてはネットワークの参加者の中から最も早く適切なナンズ⁵を計算したものがブロックを生成し、報酬として暗号資産を得ることができる。計算が最も早ければ誰であれブロック生成をするチャンスがあるというルールになっている。このように万人に開かれたブロックチェーンはパブリックブロックチェーンと呼ばれるが、多くの参加者により膨大な計算が実行されるために消費電力が多くなり、ノード数が増大するにつれてデータ通信量も増大することから、システム全体における処理性能やシステムの拡張性上の課題が生じることがある。

Ethereum は次の大規模アップグレードでは PoS(Proof of Stake)をコンセンサスアルゴリズムとして採用予定で、PoS は ETH⁶をより多く保有しているノードが優先的にブロックを生成する。PoS では、暗号資産を多く所有していることがネットワークへの貢献となりアドバンテージになるほか、現在 PoW で起きている激しい競争が緩和されて消費電力が下がることや、ブロック生成が早くなって短時間でより多くの取引を成立させられることが期待されている。

パブリックブロックチェーンが万人に利用されることを想定しているのに対して、プライベートブロックチェーンは企業間取引においての親和性が高い。中でも、ネットワークへの参加に許可が必要なパーミッションチェーンである Hyperledger Fabric や Corda では、承認する役割を予め決められたノードが承認を行うコンセンサスアルゴリズムが採用されているため、関係者内で運用できることや、承認まで短時間で済むメリットがある。

コンセンサスアルゴリズムは台帳の共有範囲や取引成立速度に関わるため、ビジネスにおけるブロックチェーンプラットフォーム選択時の検討ポイントとなる。

(3) スマートコントラクト

ブロックチェーンにはスマートコントラクトと呼ばれるブロックチェーンプラットフォーム上で実行可能なプログラム機能が備わっているものがあり、交換や契約を可能とする。取引の発生などをトリガーにしてプログラムを自動実行することが可能であり、「送金されたらアイテムを送る」といった取引や、「設定した複数の条件が満たされたときにプールした暗号資産を分配する」などのプログラムを実行することができる。例えば、ブロックチェーンを使ったゲーム「CryptoKitties」では ETH を支払うことをトリガーに可愛い猫のアイテムをランダムで獲得することができる。

保険分野でもスマートコントラクトの事例が見られる。ドイツの分散型保険アプリケーション開発企業である Etherisc の保険プラットフォームにおいては、飛行機の欠航・遅延保険のサービスが提供されている。乗る予定の飛行機情報を入力して保険料の支払いをすると簡単に加入できる。その飛行機に欠航・遅延があった場合、Etherisc が「FlightStats」等の飛行機の運航状況を参照しているために、自動的に保険金が支払われる仕組みとなっている。スマートコントラクトにより、被保険者が保険金を申請せずとも保険システムが適切に成立しているのである。

3. コンソーシアム内での効率化・コスト削減

ブロックチェーンの特性が組み合わさると、立場の異なる関係者間を何度も行き来するような契約やワークフローをオンラインで完結可能としていくことが考えられる。これによってまず期待できるのがプロセスの効率化・コスト

⁴ ヴィタリック・ブテリン氏によって開発されたブロックチェーンプラットフォーム。

⁵ ナンス (Nonce) とは使い捨てのランダムな値のことである。PoW においては、ハッシュ関数の出力を「先頭にゼロが並ぶ小さい値」へと導くナンズ値が求められる。

⁶ Ethereum プラットフォームで使用される暗号資産の単位

削減である。

IBM と Maersk が共同開発した国際貿易におけるブロックチェーンプラットフォーム「TradeLens」は輸出入におけるプロセスをオンラインのみで完結させるものであり、効率化・コスト削減をもたらしている。輸出入の各種申告や各種許可に船会社や港湾、税関、保険会社など多くの関係者が書類作成を要する。国際貿易における申請や請求の手続きは主に紙ベースで作業されており、申請内容や記載にミスがあれば書類が作成者まで遡って戻されてしまう煩雑なプロセスとなっている。「TradeLens」はこれら書類の提出・更新・閲覧をブロックチェーン上で実行可能にするものであり、ベータ・プログラムでリリースされた付属のスマートコントラクトモジュール「ClearWay」は、必要な貿易書類を受理すると自動的に輸出入許可を出すことができる⁷。

オンラインでの契約完結と、その契約記録が信頼できる状態で維持できるというブロックチェーンの効率化・コスト削減の可能性には、煩雑な業務プロセスを抱える各業界が期待を込めて課題解決に取り組んでいる。IBM は他にも、大量廃棄や偽装、衛生面の安全性などの問題によりプロセスが複雑化している食品サプライチェーンへの「IBM Food Trust」、Lenovo やノキアがネットワークに参加するサプライヤー管理・検証などのコストを削減する目的の「Trust Your Supplier」のサービス提供を始めている。

ブロックチェーン実装に伴う期待が効率化やコスト削減となっているのは、その成果を測りやすいことに加えて、限られたネットワークの中でも成果が出やすいという点にもある。「TradeLens」のプラットフォームである Hyperledger Fabric はエンタープライズ向けブロックチェーンとして適切な可視性を有しながら、データ共有を限られた参加者の中に限定する機能を有しており、コンソーシアムのような限られた関係者間でも効率化・コスト削減の効果が期待できている。ブロックチェーンの社会実装は、まずはプライベートチェーンを用いた企業間取引や限られたコンソーシアム内で効率化・コスト削減の効果をもたらすところから進みつつある。

4. 競争領域での協調による得難い価値

ブロックチェーンの普及は段階を経て社会実装に繋がっていくと考えられる。最初の段階が Bitcoin などの暗号資産の取引に始まり、次に inB（企業内）、BtoB（企業間）において効率化・コスト削減などの短期間のうちに出る成果による普及の段階があり、その先には高付加価値のブロックチェーンが普及する段階を迎えるだろう。高付加価値のブロックチェーンとは、ブロックチェーンにデータを記録すること以上の価値を新たなサービスやソリューションに付与するものといえる。例えば、機密情報である競争領域のデータを競合他社間でもブロックチェーンで共有し活用できるような新たなデータ共有の形を実現するシステムなどである。創薬においてこの事例はすでに出現している。

製薬会社は各社で化合物ライブラリーを所持しており、機械学習をライブラリーへ活用することで新たな薬の研究・開発が進められているが、一組織だけのライブラリーでは分析結果の正確性に欠けると考えられている。だが、化合物ライブラリーのデータは機密情報であり製薬企業の競争力でもあるため、競合他社に対し秘匿を解くことはできないデータである。

「MELLODDY (Machine Learning Ledger Orchestration for Drug Discovery)」は、化合物ライブラリーのデータを各社で秘匿状態を維持しながら、コンソーシアム間で機械学習に利用することができるプロジェクトである。本プロジェクトは EU における医薬品研究のイニシアチブ「IMI (Innovative Medicines Initiative)」において遂行されており、コンソーシアムにはアステラス製薬、アムジェン、メルクなどの製薬大手が参加している。技術提供パートナーである Owkin が提供する「Substra」には Hyperledger Fabric をベースとしたブロックチェーン機能が適用されて

⁷ <https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution>

いる。

「MELLODDY」はブロックチェーンとフェデレーションラーニング⁸を採用することで、秘匿された他社のライブラリーからも学習結果を集めることができるため、膨大なデータが相互に作用して創業の大きな進歩が期待されている。さらには、利用が進むにつれて類を見ない量の情報が取引され、コンソーシアムブロックチェーンの台帳へ蓄積されていくことになる。この蓄積されたトランザクション情報も見逃せない高付加価値の一つとなる。

ブロックチェーンに蓄積されたデータが機械学習分野の手法によって解析されるケースのように、データを中心とした複数の技術の融合は、競争領域での協調といった得難い価値を社会にもたらすと考えられる。

【推奨事項】

- ◆ ブロックチェーンの高付加価値創出のステージを見据える
- ◆ 競争領域のデータを活用すべく、競合他社とのコンソーシアムを組織する
- ◆ コンソーシアムに蓄積されるデータを活用すべく、フェデレーションラーニング等の他の技術とブロックチェーンを融合させる

【お問合せ先】

独立行政法人情報処理推進機構

社会基盤センター イノベーション推進部 先端リサーチグループ

E-mail : ikc-ar-info@ipa.go.jp

電話 : 03-5978-7522

⁸ 学習データを集約することなく各エッジに分散させたまま各エッジにおいて学習を行い、学習の結果のみを集約し最終結果を返す機械学習方法。