フィンテックの基礎知識

第２回 ブロックチェーンとは

デロイト トーマツ コンサルティング合同会社
デロイト エクスポネンシャル　執行役員　荻生 泰之
銀行証券ユニット　マネジャー　赤星 弘樹
銀行証券ユニット　シニアコンサルタント　宇田 陽香

ブロックチェーンとは

ブロックチェーン技術はビットコイン発祥の技術であり、P2P（ピア・ツー・ピア：端末間同士の直接通信）で接続された複数コンピュータが分散型データベースを持ち、かつコンセンサスアルゴリズム（特定の管理者なしにネットワーク参加者が取引の正しさを合意できる仕組み）を備えていることに特徴がある。取引はブロックという単位で記録され、新たなブロックが過去のブロックに鎖のように連なることからブロックチェーンと呼ばれている。

ビットコインの世界（以下、ビットコインのブロックチェーン）では、参加者間の取引はその都度ネットワーク全体に送信され、各自が保持するデータベース（過去の取引履歴）との照合により二重払い等の不正がないかの検証が行われる。その後、ブロックの生成という取引の承認作業を経て、取引の完了がネットワーク全体で合意される（図表１：ブロックチェーンの特性と従来型システムの比較）。

図表１　ブロックチェーンの特性と従来型システムの比較

従来型システム	可用性	機器の故障・ネットワーク瞬断等による一部機能停止や、大震災等災害によるシステム全面停止時に対応するためのバックアップが必要	信頼性を高い水準で確保するためには、多額の投資（システム/業務両面）が必要
	改ざん耐性	セキュリティ脆弱性を狙ったサイバー攻撃や、内部不正による記録内容の偽造等の脅威あり	
ブロックチェーン	可用性	分散型データベース（同一データを分散して保持する仕組み）のため全ノードが故障しない限り、システムは稼働可能	ブロックチェーンの特性により、高い信頼性を、比較的安価に実現可能
	改ざん耐性	コンセンサスアルゴリズムの仕組み（参加者による合意）により、悪意あるユーザによるデータ改ざんは実質的に困難	

（出所）デロイト トーマツ コンサルティング 作成

P2P の分散型データベース

ネットワークの一部が壊れても稼働し続けるために、一連のデータの複製を参加者全員が保持する仕組み。

可用性を限りなく高めるためにはプラットフォームが分散している必要があり、ハードウェア分散や地理的な分散、もしくは地政学リスクの分散のために、国境をまたぐプラットフォームを構築する方がより安定して稼働する可能性を持つ。

コンセンサスアルゴリズム

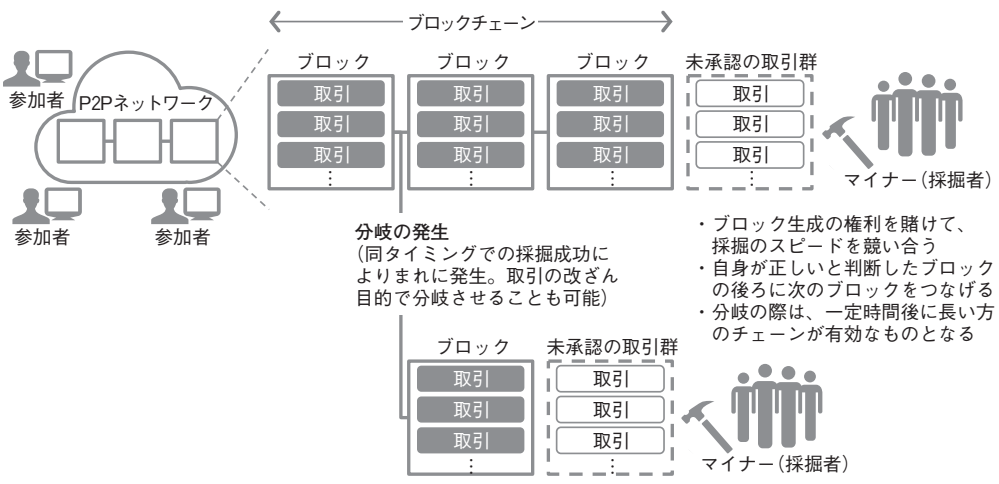
主要なもので「プルーフ・オブ・ワーク（PoW：Proof of Work）」、「プルーフ・オブ・ステーク（PoS:Proof of Stake）」、「プルーフ・オブ・インポータンス（PoI：Proof of Importance）」、「プラクティカル・ビザンチン・フォルト・トレランス（PBFT：Practical Byzantine Fault Tolerance）」の４種類がある。

（PoW とは）

ビットコインのブロックチェーンが採用する仕組み。トランザクションを承認する参加者はマイナー（採掘者）と呼ばれ、彼らにより承認されたトランザクションはブロックという単位でまとめられ、これが鎖状につなげて記録されることによりブロックチェーンが形成される。複数のマイナーにより同タイミングでブロックがつなげられるとブロックチェーンが分岐するが、分岐後に一定数のブロックがつなげられた方のブロックチェーンを覆らないものとみなし、一方で短い方のブロックチェーンに属しているブロックは破棄され、無効となる（そのために取引確定のためには一定の時間を要する）。

ブロックの生成にはマイニング（採掘）という、単純だが非常に多くのコンピュータ・リソースを要する作業が必要となるため、悪意のあるマイナーが意図的に不正なブロックチェーンを伸ばして、これを正当化するためには膨大なコンピュータ・リソースが必要となり、事実上改ざんは不可能といわれている（図表２：プルーフオブワークの仕組み）。

図表２　プルーフオブワークの仕組み



（出所）デロイト トーマツ コンサルティング作成

（PoS/PoI とは）

PoS は PoW を応用したコンセンサスアルゴリズムである。コインの保有量・保有期間が大きいほどマイニングの難易度を低くすることで、PoW に見られるコンピュータ・リソースの無駄遣いを改善している。

PoW・PoS を応用したコンセンサスアルゴリズムが PoI である。コインの保有量・保有期間の大きさに加え、直近の使用頻度が高いほどマイニングの難易度を低くすることで、PoS において想定される大量コインの保有者によるコインのため込みを是正している。

（PBFT とは）

通信ネットワークを構成する各端末（以下、ノード）のうち、特定のノード（以下、検証ノード）にブロックの生成権限を集中させ、検証ノードによる合議制 においてトランザクションの承認を行う仕組みである。コアノードは信頼できる機関により運営される必要があり、PoW・PoS・PoI のように「特定の管理者を介さずに合意形成が成立可能」といった特徴は持たないが、迅速かつ確実な取引が実現でき、単一企業での取引（プライベート型）や複数企業・団体での取引（コンソーシアム型）といった特定の参加者内での活用が期待されている（図表３：コンセンサスアルゴリズムの種類と特徴）。

ブロックチェーンの適用領域

ブロックチェーンの技術特性は一般的に、高透明性・高信頼性・高効率性と言われ、金融業においては幅広い領域で活用可能である。特に、経済活動の基盤となる金融インフラにブロックチェーン技術が適用された場合、技術革新の恩恵を幅広く享受することが可能になる（図表４：ブロックチェーン技術特性と適用領域）。

実証実験と実用化状況

（国際的なコンソーシアム）

最初に挙げられるのがスタートアップ企業

図表３　コンセンサスアルゴリズムの種類と特徴

		PoW	PoI・PoS	PBFT	
特徴	参加形態	パブリック型 （誰でも参加可能）		コンソーシアム型 （特定の複数企業・団体）	プライベート型 （特定の単一企業）
	可用性	全てのノードにブロックの生成権限があるため、１ノードでも稼働していれば継続運用が可能		ブロックの生成権限をコアノードに集中させるため、一定数のコアノードが停止した場合に継続運用が不可	
	ファイナリティ	複数のノードが同タイミングでブロックを生成した場合、ブロックが分岐し取引が無効になる可能性		検証ノードによる合議において１つのブロックが生成されるため、ブロックは分岐せずファイナリティ確保が可能	
	性能	ブロックの生成に一定程度の難易度を設ける必要があり、その分、トランザクションの承認には時間が必要		ブロックの生成は信頼できるコアノードのみで実行されるため、比較的短時間でのトランザクション承認が可能	
適用例		ビットコイン、イーサリアム（注１）等 仮想通貨		ハイパーレジャー（注２）等 企業取引	

（注１）種々のアプリケーションを構築するためのプログラミング言語を備えたプラットフォームであり、イーサという通貨を持つ（ビットコインの次に時価総額が大きい）。
（注２）取引の記録と検証を行うためのブロックチェーン技術を推進するオープンソース・プロジェクト。
（出所）各種情報を基にデロイト トーマツ コンサルティング作成

図表４　ブロックチェーン技術特性と適用領域

技術特性

高透明性
・承認されたデータは全ての参加者が同時に参照可能
・一度合意したデータが遡及的に変化しない（改ざんできない）

高信頼性
・一部のノードが故障しても、他のノードが生存している限り応答し続ける
・ノード間のネットワークが障害等で分断されても、システムがダウンしない

高効率性
・処理分散によるシステムコスト低減
・障害時のメンテナンスコスト低減
・契約・決済を扱う業務のスピードアップ・事務コスト低減　等

処理速度、セキュリティの面での課題もあるため、今後更なる研究を重ね、課題を解消する必要性あり

適用領域

分類	想定される適用領域
金融サービス	・仮想通貨 ・ポイント ・国際送金 ・貿易金融 ・シンジケートローン ・金融商品取引 ・債権発行 ・ポストトレード
金融情報管理	・KYC（注３） ・個人情報管理 ・信用情報管理 ・契約管理

（注３）know Your Customer（顧客確認）の略。新規口座を開く際に要求する書類手続き等の総称であり、金銭の不正使用の防止等を目的としたもの。
（出所）各種情報を基にデロイト トーマツ コンサルティング作成

である R3CEV 社が主導する R3コンソーシアムである。このコンソーシアムには世界の大手金融機関が70社以上参画しており、金融機関のブロックチェーン・プラットフォームを作ることを目的としている。これ以外にも、大規模なコンソーシアムとして Linux 財団と日米欧の銀行・IT ベンダー等の Hyperledger プロジェクト等がある。ブロックチェーン技術の世界的な主導権争いが起こっている。ブロックチェーンは期待感が極めて高い一方で、まだ研究開発中で新しい仕組みが日々生まれるため、引続き技術動向を見極める必要がある。現に R3の直近報道では一部主要銀行の離脱表明や、主要製品である Corda（コルダ）は厳密にはブロックチェーンではないといった発言も顕在化した。

（国内のコンソーシアム）

国内でも動きがある。３メガバンクとデロイト トーマツ グループは、銀行業界全般への貢献の理念の下、ブロックチェーン研究会を設立し銀行間振込業務の実証実験を公表。また、直近では第２フェーズの取組が開始されている。この他には SBI リップルが国内外為替の一元化検討に関するコンソーシアムを、地域金融機関やインターネット専業銀行等を含む42行と発足している（図表５：各コンソーシアムの概要と直近動向）。

（個別取組例）

金融業におけるブロックチェーン技術の適用は実証実験に留まらず、実用化に発展しつつある。国内でもメガバンクを中心に個別行あるいは複数行が共同し実証実験を行っているが、国外の一部では実験に留まらず実用化事例も出ており、2017年度は実用化元年といわれている。今後、更なる実用化の波が押し寄せ、顧客が利便性・コスト効率性の恩恵を受ける日が迫っていることに疑う余地はない（図表６：ブロックチェーン技術の実用化状況）。

図表５　各コンソーシアムの概要と直近動向

名称（設立年月）	参加行	概要	直近動向・実績
R3 （2015年９月）	・ブロックチェーン技術を有するR3CEVと、日米欧の70社以上が参加 ※ゴールドマンサックス、サンタンデール、モルガンスタンレー銀行等離脱	・グローバル金融機関向けに、ブロックチェーンのメリットを活かした金融取引インフラを開発すること	・金融向け契約管理プラットフォームコーダを発表 ・40行との間で債券取引の共同実験を実施、15行との間でトレードファイナンス分野でプロトタイプを開発等、複数の実証実験を実施中
ブロックチェーン研究会 （2015年12月）	・三菱UFJフィナンシャル・グループ ・みずほフィナンシャルグループ ・三井住友銀行 ・デロイト トーマツ グループ	・ブロックチェーン技術の研究により実用化の方向性を定めることで、国内金融業界の発展に寄与すること	・ブロックチェーンによる国内送金の実証実験を行い、全銀システム並の秒間1,500件の処理能力が実現できることを確認 ・引続き、ブロックチェーン技術を適用しうる銀行業務を選定し、検証を実施（予定）
ハイパーレジャー （2016年２月）	・非営利団体Linux財団が中心となり、米欧の銀行・SIer・ベンチャー企業等、世界30以上の先進的IT企業が参加	・ブロックチェーン技術/P2P分散レッジャー技術を確立	・オープンソースの考え方に基づいて、グローバルレベルで共同検証を実施し、デファクトスタンダードとなるブロックチェーン基盤の技術開発/推進 ・Fabric（IBM）、Sawtooth Lake（インテル）、Iroha（ソラミツ）を正式に受諾し推進中
W3C （2016年８月*） *Blockchain Community Groupの設立	・Web技術に関わりの深い企業、大学・研究所、個人などで構成	・Blockchain Community Groupを設立 －ブロックチェーンに関連する新しいテクノロジーの評価や、銀行間取引のようなユースケースを検討	・メッセージフォーマットの標準化を目指しガイドライン作成（予定）
SBIリップル （2016年８月）	・地域金融機関、インターネット専業銀行等を含む42行が参加	・「国内外為替の一元化検討に関するコンソーシアム」を発足 －国内外為替の一元化 －24時間リアルタイム決済 －送金コストの削減と新市場の開拓	・2017年３月を目途に国内・海外送金の一元化に関する実証実験を行い、その後、分科会にて商業利用を検討（予定）

（出所）各社ホームページ等を基にデロイト トーマツ コンサルティング作成

図表６　ブロックチェーン技術の実用化状況

分類		主要な取組の傾向	実証実験例	実用化例
金融サービス	通貨	仮想通貨発行に留まらず、決済を円滑化する中央銀行向け通貨や、企業独自の通貨やポイントの発行が加速	【仮想通貨】 UBS、Deutsche、BNY Mellon、Santander	【仮想通貨】 ビットコイン
	送金・決済	決済時間の短縮が求められ即時性が必ずしも求められない「国際送金」への取組が世界中で特に活発	【国内送金】 SMBC、みずほ、MUFG	【国際送金】 Santander（Ripple）
	融資	契約条項の履歴管理や、一連の取引記録の管理として期待される、「貿易金融」や「シンジケートローン」の分野での取組が中心	【シンジケートローン】 みずほ	【貿易金融】 KBC Bank
	金融商品取引	速度を求められない未公開株取引、債券取引の実現や、業務効率化が期待されるポストトレード等の取組が中心	【ポストトレード】 BoA、Citi、JPMorgan、Credit Suisse	【未公開株取引】 Nasdaq
金融情報管理		個人情報管理、企業情報管理、KYC等、金融機関が持つ情報を統合したインフラの新規構築、既存更改	【企業情報管理】 Kompany.com	【KYC】 ConsenSys

（出所）各社公開情報を基にデロイト トーマツ コンサルティング作成

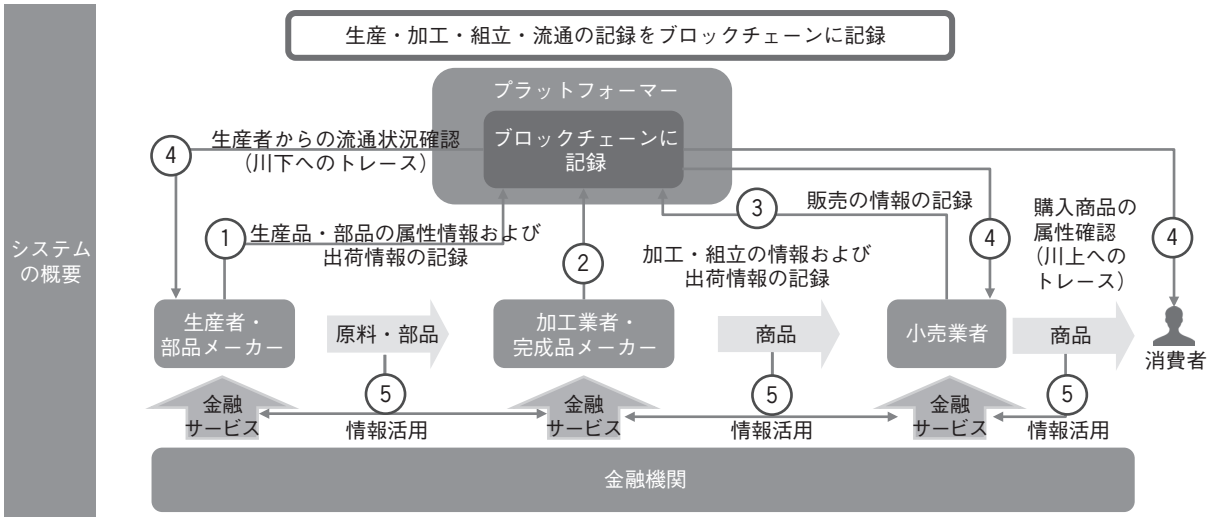
機会と脅威を踏まえた戦略の必要性

ブロックチェーンは金融業だけではなく公共（マイナンバー等）・物流・IoT 等の分野への適用も期待されている。

その中でも期待されている領域が物流・トレーサビリティへの活用である。生産者、加工業者、小売業者等が個々の商品の生産・加工・流通の情報をブロックチェーンに記録。これにより、サプライチェーンや物流の最適化、工業製品や農水産物の安心・安全性の確保、決済システムとの連携による企業活動の効率化が期待される。今後金融機関がこれらの取組に深く参画する事でデータを活かした金融サービスの高度化が期待できる一方、プラットフォーマーが大手の製造業者、小売業者、総合商社、IT 事業者である可能性もあり、商流ファイナンスのサービスを奪われる脅威も考えておく必要がある。例えば、ブロックチェーンではないが、中国のアリババグループは IT 事業者でありながら電子商取引プラットフォームに留まらず金融プラットフォームと物流プラットフォームも展開し、出店する零細事業者に対して効率的に貸付を行う仕組みを構築している。今後はこの様な前例を基にブロックチェーン技術によるプラットフォーマーとしての参入も考えられる。

ブロックチェーンの研究開発は進み、徐々に実用化に向けて動き出していく中では、残る課題も多い。ただし、ブロックチェーンが革命を起こす可能性を秘めた技術であることは間違いなく、金融機関においては先を見据えた先手の戦略、リスクへの備えが求められている（図表７：物流・トレーサビリティへのブロックチェーン技術の活用～実現イメージ）。

図表７　物流・トレーサビリティへのブロックチェーン技術の活用～実現イメージ



（出所）デロイト トーマツ コンサルティング作成