いまさら聞けないブロックチェーンの基礎知識と実装の要件

本稿では、オープンスタンダードな環境をメインフレームで動かすことのメリットを掘り下げていきます。今回は今話題のブロックチェーンについて、まずは「ブロックチェーンとは何なのか」「ブロックチェーンを実行する基盤に求められるものは何か」、そして「既存のビジネスモデルの何を変え得るのか」を整理していきます。これを理解することで、メインフレームLinuxが皆さんの業務や事業にとって大きな意味を持つことが理解いただけることと思います。

1. そもそもブロックチェーンとは

「ブロックチェーン」と「ビットコイン」(注1)は同じレイヤーの用語として考えられがちですが、実のところ、「ブロックチェーン＝ビットコイン」ではありません。ブロックチェーンはあくまでも基盤技術であり、ビットコインは「ブロックチェーン技術で実現されるアプリケーション」です。

(注1) ビットコイン（Bitcoin）：インターネット上で取引や通貨発行が行われる暗号通貨の1つ。政府や銀行などの中央機関を介さず、ネットワークの参加者間で取引が行われる

○ブロックチェーンの基礎概念

まずブロックチェーン技術を構成する重要な概念として、「台帳（Ledger）」「取引（Transaction）」「取り決め（Contract）」という3つの基礎を整理しておきましょう。

台帳（Ledger）には取引（Transaction）の結果が記録されます。ここでいう取引（Transaction）とは、例えば、「AさんからBさんに100万円が支払われた」といったものを指します。その取引（Transaction）を行うためには、ビジネス上の取り決め（Contract）が必要となります。つまり、「取り決め」に従い、「取引」を実行し、「台帳」に取引の結果を記録するというのがブロックチェーン技術で実現される処理の一連の流れになります。

ブロックチェーンを一言で言ってしまえば「台帳」を分散共有して管理する技術です。従来はビジネスネットワークに参加している参加者それぞれが台帳を管理する、あるいは第三者機関が中央で管理し、取引の正当性を保証しています。一方ブロックチェーンでは、参加者全員が同じ内容の台帳を所有し、お互いに監視し合うことで取引の正当性を保証します。

図1　中央管理型とブロックチェーン型

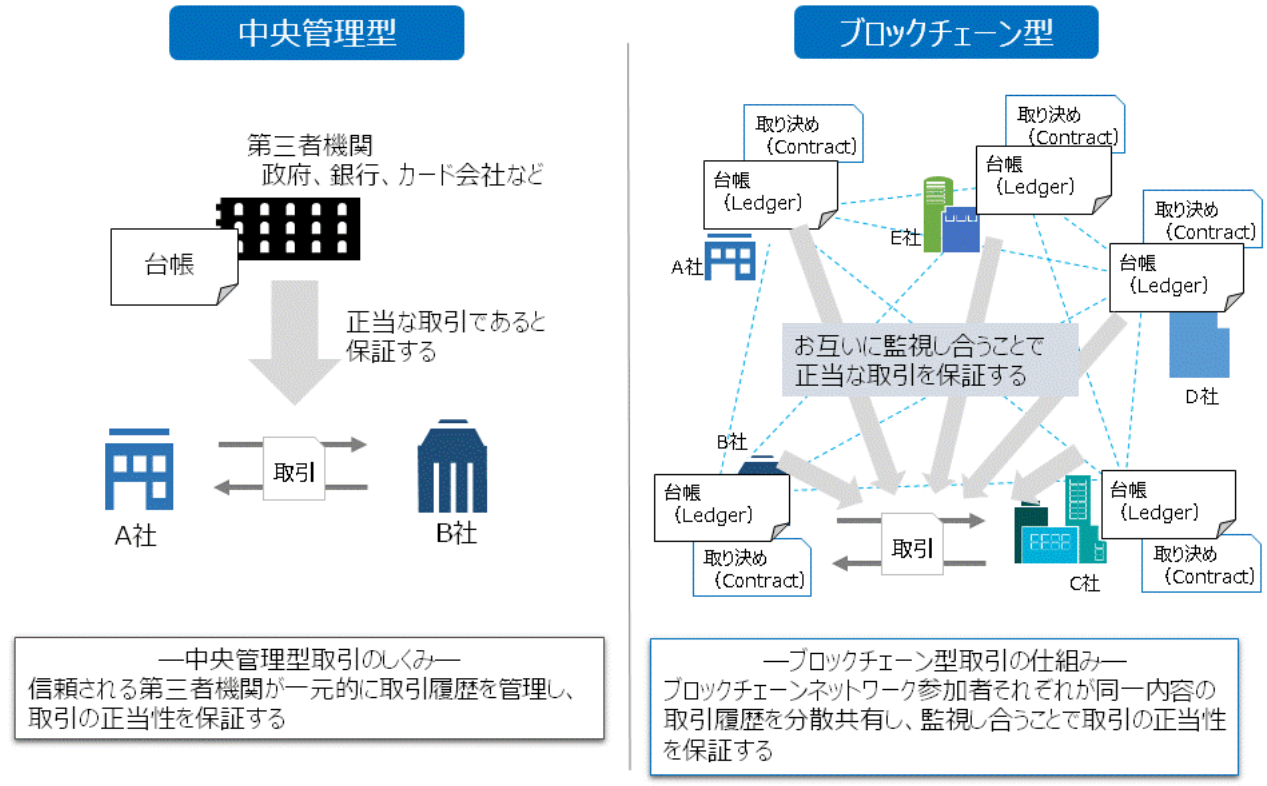
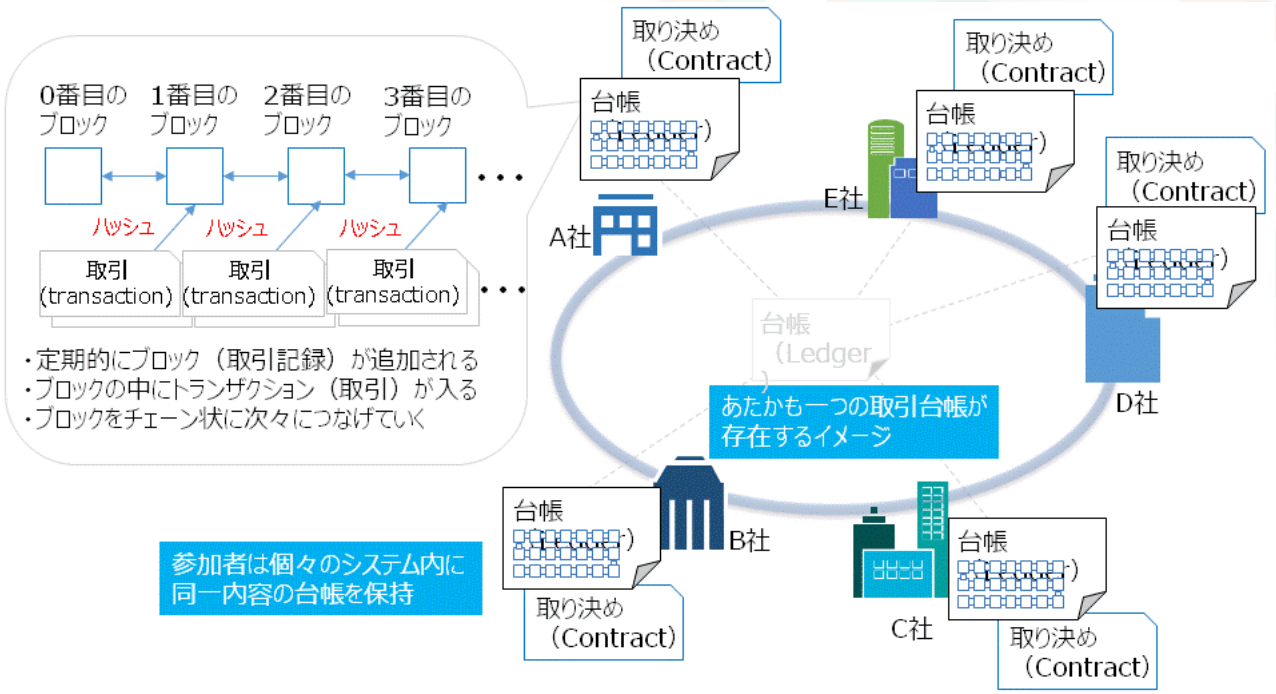


図２　ブロックチェーン全体像



ではなぜ、このような技術が注目を浴びているのでしょうか。それはブロックチェーンが各種取引の「期間」「コスト」「脆弱（ぜいじゃく）性」を改善すると期待されているためです。

例えば、輸出入を円滑に行うために必要な資金の融通を行う貿易金融では、銀行、輸出企業、運送会社、輸入企業などの多数の参加者の間で、大量の貿易書類をやりとりする必要があり、それら文書の処理に多くの手間と時間がかかっています。

貿易金融に関わる多数の企業でブロックチェーンのネットワークを構成することで、参加する全ての企業が取引情報を記録している台帳を持ち、その台帳に各企業が行う処理（取引）を書き込むことで、その処理が他の企業の台帳にも反映されます。決済指示や処理をワークフローとして自動化することができるので、プロセスの迅速化とコストの削減が期待されています。

ブロックチェーンは台帳管理を分散化することで、中央管理によって実現していた管理形態をピアツーピア[注2]で実現できるようになります。これにより取引にかかる期間やコスト（仲介手数料など）の削減が可能になり、また不正や改ざんなどをソフトウェア的に制御することが可能になります。

（注２）ピアツーピア（Peer to Peer）：複数の端末間で通信を行う際のアーキテクチャの１つで、対等の者（ピア）同士が通信をすることを特徴とする通信方式

貿易金融の例のようにブロックチェーンの活用はビットコインのような不特定多数の参加者によるパブリックな環境

図３　ブロックチェーンのネットワーク形態

	パブリック型	コンソーシアム型	プライベート型
参加者	自由 →不特定多数、悪意のある参加者を含む可能性がある	許可制 →参加者は特定されており、信頼できる	
コンセンサス方式	Proof of Work	PBFT 特定の検証者による検証	
ユースケース	Bitcoinなどの仮想通貨	銀行間送金、証券取引などのビジネスネットワーク	

だけでなく、よりビジネスでの適用性を向上させたコンソーシアム型／プライベート型といった、特定された参加者間でブロックチェーンネットワークを構成するケースもあります。

IBM はコンソーシアム型／プライベート型のブロックチェーンネットワークにおいて、標準的なブロックチェーン基盤を推進するオープンコミュニティーである Linux Foundation (注 3) の HyperLedger Project (注 4) の発足メンバー、議長として参画しています。IBM はハードウェアやアプリケーションに依存しないブロックチェーンのコアとなるコードを同コミュニティーに寄贈しブロックチェーンの標準化をリードしています。このコアとなるコードは Hyperledger Fabric (注 5) と呼ばれます。

IBM は Hyperledger Project のブロックチェーンサービスをアプリケーション開発基盤である Bluemix (注 6) 上で展開し、また、ブロックチェーン基盤に求められる信頼性、パフォーマンス、セキュリティを備える LinuxONE での適用に注力しています。

（注 3）Linux Foundation：Linux オペレーティングシステムの普及をサポートする、非営利のコミュニティ

（注 4）HyperLedger Project：Linux Foundation が中心となり、世界 30 以上の企業が協力しブロックチェーン技術を推進するコミュニティ

（注 5）Hyperledger Fabric：HyperLedger Project のベースソフトウェアとして採用されている

（注 6）Bluemix：IBM が提供する Platform as a Service の総称。日本を含む世界各地のデータセンターからサービスを提供している。さまざまなアプリケーションを構築、管理、実行するための「オープンスタンダードとクラウドをベースとしたプラットフォーム」。OpenStack や Cloud Foundry といったオープンソースソフトウェアや標準化仕様に準拠した技術を多く取り入れている点が特徴

○ブロックチェーンの 4 つの技術要素

ブロックチェーンは台帳を分散共有して管理する技術と紹介しましたが、その技術要素について詳しく紹介します。

先に、ブロックチェーン技術を構成する重要な概念として、「台帳（Ledger）」「取引（Transaction）」「取り決め（Contract）」を紹介しました。これらはあくまでも概念であり、この概念を実装する際には、具体的なブロックチェーン実装の技術要素「分散台帳」「暗号化」「コンセンサス」「スマートコントラクト」の 4 つが必要です（図 4）。以降で、それぞれの要素を見ていきましょう。

（1）分散台帳：ビジネスネットワーク上の参加者間で共有される「取引データ台帳」です。ブロックチェーンネットワークに所属する参加者はピア（Peer）と呼ばれています。ピアにはトランザクションの実行や合意形成を行う Validating ピア（バリデーティングピア）と、アプリケーションとの連係を行う Non-Validating ピア（ノンバリデーティングピア）の 2 つが存在します。

（2）暗号化：電子署名機能、認証機能により、取引の正当化や機密保持を確立するための要素です。ブロックチェーンネットワークにおいて参加者間のトランザクションは全て暗号化されます。

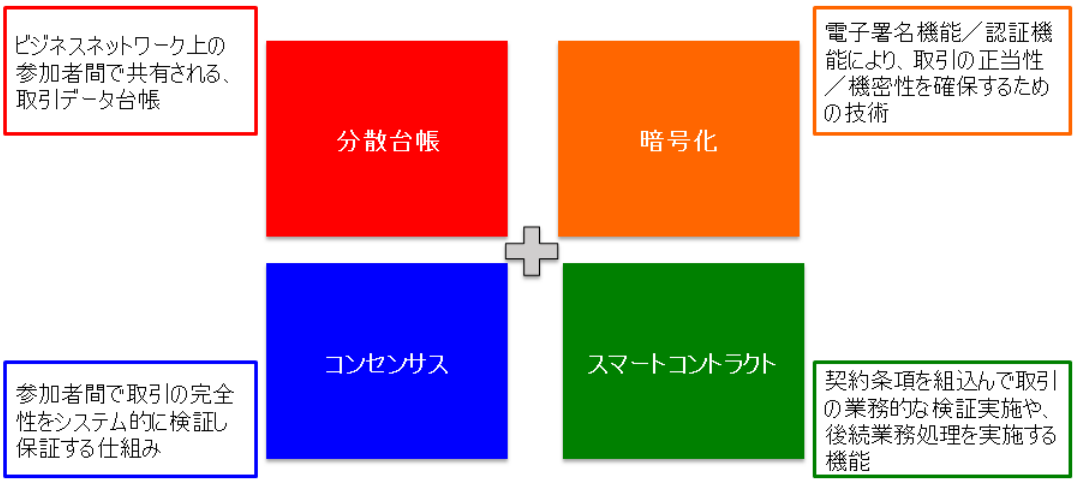
（3）コンセンサス：参加者間で取引の安全性を検証する仕組みです。参加者が持っている分散台帳に保存されている取引記録がどの台帳においても同じであるように「合意」を行います。

取引記録を一定数まとめたものをブロックと呼びます。Hyperledger Fabric での合意形成は「PBFT」(注 7) というモデルを用います。その他の合意形成モデルには、ビットコインで使われている「プルーフオブワーク（proof of work）」(注 8) などがあります。

（注 7）PBFT（Practical Byzantine Fault Tolerance）：複数の複製の間で台帳を同期するためのプロトコル。(N-1)/3 の参加者が同時に不正をしようとしても、正確な合意形成が可能な点が特徴

（注 8）プルーフオブワーク（proof of work）：不特定多数の参加者のためのブロックチェーンネットワークにおける合意形成メカニズムの 1 つ。各取引を認証するために算出しなければならないデータまたはそのようなシステム

図 4　ブロックチェーン 4 つの技術要素



PBFT ではブロックチェーンネットワークの参加者が特定されているため、少ないコストで高速に合意形成が可能です。

また、取引記録をブロックとして台帳に保存する際に、取引をハッシュ化し、前のブロックのハッシュ値を計算してそのブロックに埋め込む処理を行い、現在と過去のブロックの関連を持たせます。こうしておくことで、過去の取引記録を操作するには関連する全てのブロックの改ざんが必要となるため、実質的に改ざんは不可能といえます。このようにブロック同士の関係を計算した値として記録することで改ざんを防いでいます。

(4) スマートコントラクト：ビジネスロジックそのものであり、トランザクションが発生すると実行されるプログラムです。Hyperledger Fabric では「チェーンコード」と呼ばれます。チェーンコードはピアに配布され、トランザクションによりチェーンコードで定義した処理が実行されます。

チェーンコードの処理にはチェーンコードを登録する「deploy」、チェーンコードを実行し、台帳への書き込みを行う「invoke」、データの問い合わせ、読み込みを行う「query」があります。後述のデモではこれらチェーンコード処理を実行します。

○ブロックチェーン技術の 4 要素に必要な基盤要件とは？

では、これら 4 つの技術要素が基盤に求める要件とはどのようなものでしょうか。

(1) 分散台帳：取引情報を記録するいわば基幹システムとなるため、常に安定的なトランザクションを行え、また高い可用性を持ち、止まらない基盤が必要です。

(2) 暗号化：参加者間のトランザクションは全て暗号化されるため、高速な暗号化と復号が必要です。また証明書や鍵自体を安全に保管する必要があります。ブロックチェーンは各ノードに台帳を分散して管理するため、各ノードのセキュリティを確保する必要があります。

(3) コンセンサス：参加者間で合意形成する際、大量のネットワークトラフィックが発生するため高速なネットワーク通信が求められます。

(4) スマートコントラクト：チェーンコードはビジネスロジックのため、プログラムの改ざん防止策や既存システムとのセキュアな連係も求められます。

ブロックチェーンによって新しいビジネスモデルを作るには、これら 4 つの技術要素が求める要件を十分に満たし、基盤自体にリスクがなく信頼できるものでなければなりません。

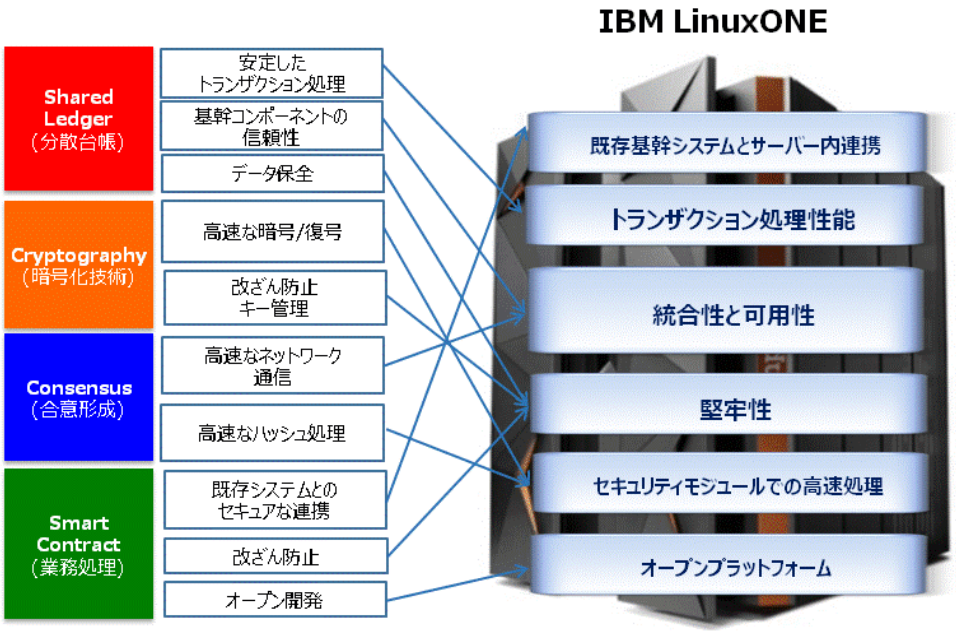
2. LinuxONEでブロックチェーンは現実的か？

ブロックチェーンの 4 つの技術要素が基盤に求めるものを満たすものが IBM の LinuxONE です。LinuxONE では次のことでメリットがあります。

- **CPU 使用率 90%を超える高負荷状態でも安定**

一般的に IA サーバは、高負荷状態になるとパフォーマンスが低下してしまうのに対し、LinuxONE は CPU 使用率 90%を超えたとしても、パフォーマンスが低下することなく、安定したトランザクション処理や高速なハッシュ処理を行うことができます。

図 5　LinuxONE でブロックチェーン



• 軍事レベルのセキュリティ機能をハードウェア的に実装

ハードウェア自体に組み込まれたセキュリティ機能により、コンピュータで唯一軍事レベルに準ずる「EAL5」(注9)のセキュリティレベルを実現します。セキュリティ事故0件の実績を持ち、改ざん防止や安全な鍵管理が可能。台帳を管理するノードが増えたとしても、セキュリティ上安全にシステムを稼働させられる能力を持っています。

(注9) EAL5:セキュリティ製品およびシステムの開発や製造、運用などに関する国際基準であるISO/IEC 15408の評価基準の規定内容の一部。EAL(Evaluation Assurance Level)はセキュリティ確保に必要な信頼性について規定されている。EAL1～3は一般民生用、EAL4は政府機関向け、EAL5～7が軍事および政府最高機密機関向けに分類されている。

• 基幹業務システムとの親和性

基幹業務システムの多くはIBMのメインフレームで動いているため、既存システムとブロックチェーンシステムをセキュアに連係可能です。

• 高可用性と高い稼働実績

平均故障間隔35年以上の実績、24時間365日稼働が可能な高い可用性により、高速なネットワークや基幹コンポーネントの信頼性を確保します。

• オープンスタンダードな開発環境

Linuxや Docker、Go言語や Node.jsなどのオープンな環境で開発が可能です。

このようにブロックチェーンの4つの技術要素に必要な基盤要件をLinuxONEは満たし、ブロックチェーンで新たなビジネスモデルを確立するための最適な基盤といえます。

著者：栗村 彰吾

さまざまなオープンソースソフトウェア（OSS）に携わり、現在は「LinuxONE」を中心に、提案および構築を担当。お客さまのミッションクリティカルな業務にふさわしいシステムの提供に尽力する傍ら、LinuxONEの活用に関するセミナー講師として「メインフレームの価値」や「なぜ今メインフレームか」を啓蒙する活動にも従事する。

お問い合わせ先▶ **日本アイ・ビー・エム株式会社** 〒103-0015 東京都中央区日本橋箱崎町19-21 http://ibm.biz/linuxone_jp
IBMアクセスセンター 0120-550-210

※この冊子は、キーマンズネット（http://www.keyman.or.jp/）に2016年10月に掲載されたコンテンツを一部改訂・再構成したものです。 http://www.keyman.or.jp/kc/30009281/