

これから注目の「分散型」 ブロックチェーンの基礎知識

佐藤 聖

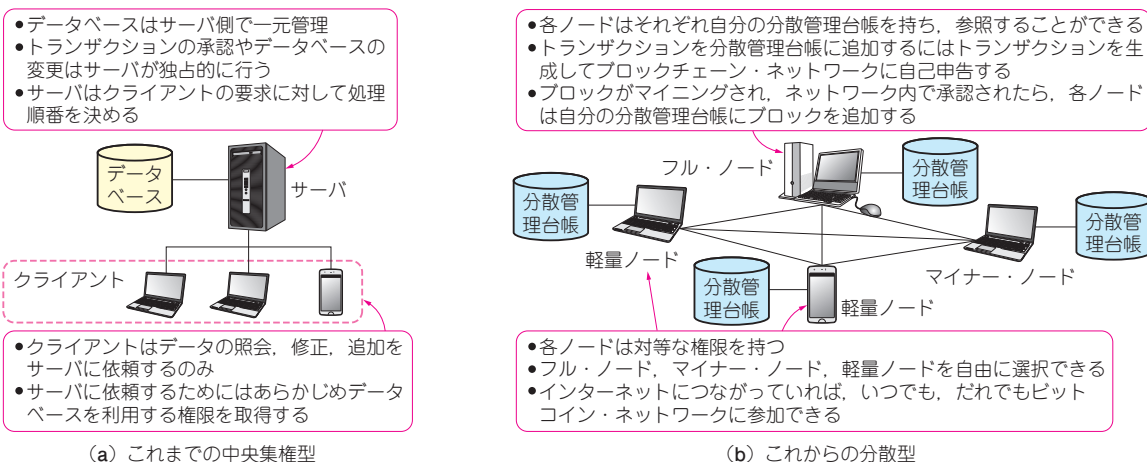


図1 これからのネットワークは「分散型」が注目

知っておかないとマズい理由

ブロックチェーンが話題になる理由は、画期的プラットフォームだからです。このプラットフォームでは、お金の取引だけでなく、あらゆるデータの収集や記録に利用できるため応用範囲が広く、あらゆるビジネスにも影響を与える可能性があります。

プラットフォームは一度普及すると発電事業や道路事業のように長期間インフラとして利用されます。そのため世界中でブロックチェーンによるプラットフォームが開発され、事実上の業界標準として認知されるよう、覇権をめぐる競争が繰り返されています。

ブロックチェーンはいろんなネットワーク技術を積み重ねたものであるため(詳細は後述)、暗号通貨ではないIoT的な使い方に注目! といながらも、暗号通貨という言葉が出てきてしまうのは説明上許してください。

一番の特徴… ネットワークにサーバが要らない

● 従来の中央集権型

従来の中央集権型データベース(図1)は、Tポイン

t, Ponta, 楽天ポイント, dポイントなどのポイント・システムや, Suicaなどの電子マネー決済システムに利用されています。こうしたシステムは運用会社が存在し、管理者によってデータが管理されています。

中央集権型データベースの代表例として、リレーショナル・データベースがあります。コンピュータでデータを「保存・編集・参照」するためには、Oracle, SQL Server, DB2, MySQL, PostgreSQLなどのデータベース管理ソフトウェアがあります。データベースの台帳機能は基本的にテーブルが担っており、関係モデルを表現しています。データベースはデータを記録するだけでなく、加工や参照にも利用されます。

中央集権型データベースは、サーバ障害や通信障害によってサービスが停止してしまうと、クライアントからデータ操作ができなくなります。一元的に管理するため障害が発生しても復旧まで短期間で対応されるよう、事前に障害対策が施されていることが一般的です。

● これから注目の分散型

ブロックチェーンのデータはPeer to Peer (P2P) ネットワーク、分散型タイム・スタンプ・サーバに

表1 ブロックチェーンはいろいろなネットワーク技術を組み合わせて実現する

ブロックチェーン	主な用途	主要アプリケーション	主要ブロックチェーン技術	機能
1.0	暗号通貨	ビットコインの取引をサポートするプラットフォーム	ブロックチェーン	暗号通貨のP2P取引
		アルトコインの取引をサポートするプラットフォーム	アルトチェーン	
2.0	デジタル情報取引	スマート・コントラクトに代表されるデジタル・アセット	カラードコイン	Open Assets Protocol (権利情報) など
			パーミッションチェーン	参加者の権限設定など
			サイドチェーン	異なるブロックチェーンを連携させる
			マイクロペイメント	トランザクションはブロックチェーン外で処理し、ブロックチェーンにコミットすることでパフォーマンスとコスト効果を得る
3.0	ブロックチェーンのプラットフォーム化やサービス化	ブロックチェーン・サービス (BaaS)	上記を含む	ブロックチェーン上にアプリケーションを構築

よって自律的に管理されます。中央集権型データベースのように管理者がいなくても特徴です。

ブロックチェーンでは、データの取引を認証するための組織や管理者が存在せず、自立的に管理する仕組みが備わっています。

ブロックチェーンにはサーバが存在しないため、サーバ障害がなく、通信障害が発生したとしても一部のノード(マイナーのコンピュータ)にしか影響せず、全体に障害の影響が波及しません。逆に言うとインターネット上のどこかのネットワークに接続しているノードに障害が発生しても、常に全体として機能するように考慮されています。

万が一、ノードやネットワークに障害が発生しても、正常に稼働しているノードだけでトランザクションの作成、マイニング、トランザクションの認証などが進むので、データの取引全体が停止することがありません。

インターネットによる通信は専用線や地上電話ほど安定していません。ハードウェア障害、トラフィック

量の急増、サイバー攻撃などで通信できなくなることがよくあります。ブロックチェーンでは中央管理のデータベースよりも障害に対する高い耐性があります(4)(5)。

技術の階層

ブロックチェーンは、分散型台帳技術、分散型ネットワーク技術と呼ばれ、用途や機能の違いでブロックチェーン1.0、2.0、3.0があります(表1)。各バージョンの定義は組織やプロジェクトで異なりますがおおよそ次の通りです。

- ブロックチェーン1.0…暗号通貨への応用で支払い機能に特化
- ブロックチェーン2.0…暗号通貨以外への決済用途等で利用される。契約の自動実行(スマート・コントラクト)機能(図2)など
- ブロックチェーン3.0…金融以外の分野でのIoTや人工知能と組み合わせた応用(ブロックチェーン2.0を含む)

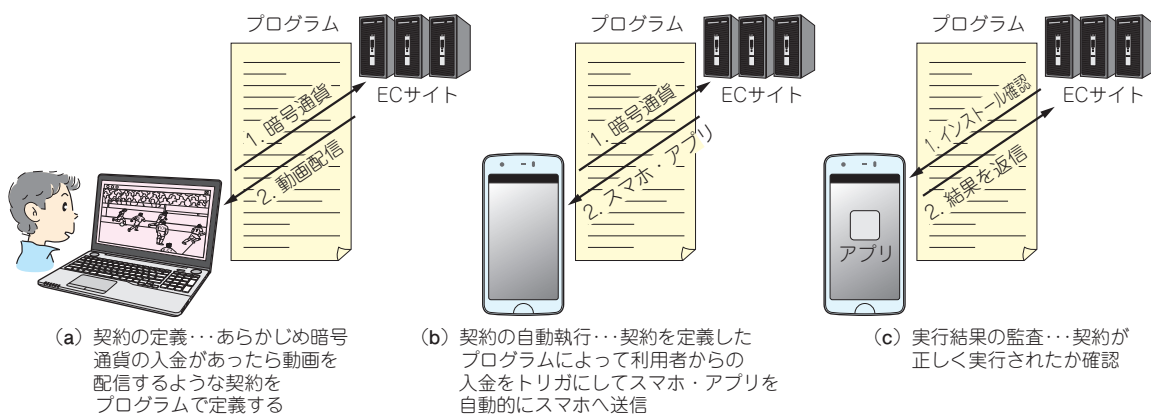


図2 契約の自動実行機能(スマート・コントラクト機能)がベースになると簡単に安全なやりとりが可能になる