TOSHIBA

プライベートブロックチェーン

～プライベートブロックチェーンを活かしたオープンなコミュニティの場の創出～

**様々な分野で、自社の垣根を越えたデータの利活用が求められています。
東芝では、アプリケーションとアプリケーションをつないで、自由でかつ透明性のある
データ流通の場の創出をブロックチェーンで実現します。**

東芝デジタルソリューションズはこれまでも複数サーバーで高信頼なシステムを実現するクラスタシステムを扱っており、そこで培った技術を基に、高速で可用性・信頼性に優れたブロックチェーンの実現を目指しています。

既存のデータ流通の課題

- 自社が持つデータで新たな販路を拡大したい
- 自社の事業に有益なデータを手間を掛けずに入手したい
- 自社データが誰にどのように利用されたかを知りたい
- データの所有権を明確化したい
- 取引ルールや取引結果の透明化を図りたい

特徴

東芝が描くブロックチェーンを活用したマーケットプレイス

利用目的毎にアプリケーション連携の場（マーケットプレイス）を創出

利用目的毎にマーケットプレイスを創出し、データ提供するアプリケーション、データ活用するアプリケーションが自由に参加できる

ブロックチェーンによる取引履歴の管理

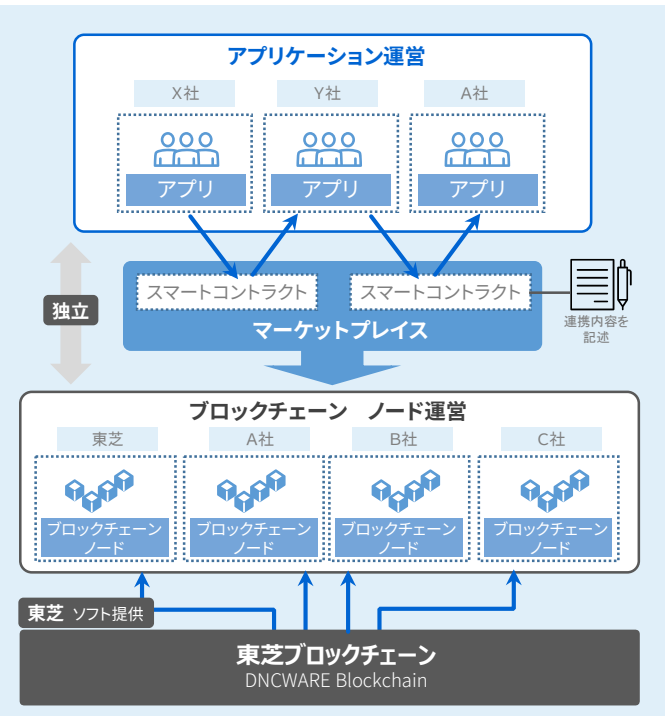
連携の記録は全てブロックチェーンで記録され、改ざんが困難
記録の検証や監査にも対応可能

連携内容はスマートコントラクトによって記述

ビジネスモデルに応じて、スマートコントラクトで連携内容を記述
連携内容の登録・変更にノード運営側は関与する必要はない

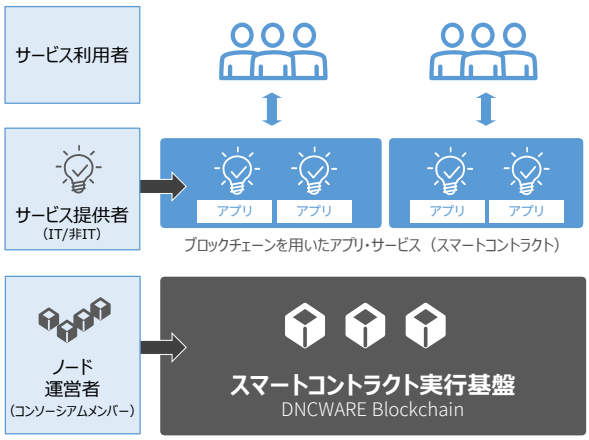
アプリケーションだけ、ノードだけの参画が可能

アプリケーション運営とノード運営が独立しているので、アプリケーションだけ（X社、Y社）、ノードだけ（B社、C社）、両方（A社）のような参画が可能



プライベートブロックチェーン　DNCWARE Blockchain [ディーエヌシーウェア ブロックチェーン]

プライベート型のスマートコントラクトの実行基盤
ブロックチェーンを利用したアプリケーションサービスを素早く立ち上げ可能



サービス提供者は、ブロックチェーンの存続の心配やその運営に煩わされずに、アプリ・サービスを提供可能

- コンソーシアムで運営する信頼あるブロックチェーンの上に、アプリ・サービスのスマートコントラクトを展開可能。
- アプリの展開にはコンソーシアムの関与なしで可能。
- 透明性の確保。アプリの作成・変更、アクセス権の設定がすべてブロックチェーンに記録され、誰が作成・変更したのかがわかる。

ブロックチェーンをコンソーシアムで運営アプリ・サービスをノード運営とは独立に提供可能

- コンソーシアムでのノードの運営が可能。
- 信頼あるメンバーで運営・ノード維持の信用。改ざんなどの不正は困難。検証による相互監視。
- アクセス制御により、アプリ・ユーザを保護。

技術・開発面での特徴

すべての変更を記録
スマートコントラクトの呼び出し（リクエスト）だけではなく、コントラクトの変更や、権限の変更、システム構成の変更などがすべてブロックチェーンに記録されます。システム管理者やアプリケーション開発者の行動もすべて記録されます。

記録の改ざんが困難
電子署名により第三者による改ざんが検出可能です。ブロックチェーンにつなぐことにより、当事者がトランザクション再発行改ざんが検出可能です。コントラクトは分散環境で冗長化して実行・結果が比較されるため、ビア管理者による実行の改ざんも検出可能です。トランザクションが改ざんされていないことを証明する検証データを出力可能です。

高可用性と高信頼性の両立
データおよび実行を分散して多重化し、高い可用性を実現しています。Ben'Or型の合意形成アルゴリズムで、PoW(Proof of Work)よりも格段に高速で、かつ、一貫性のあるビザンチンフォールト耐性を備えた高信頼を実現しています。

アプリケーションの開発が容易
汎用のJavaScriptで記述ができるため、習得が容易です。ウェブ開発経験者など開発者の確保がしやすくなります。また、コンパイル不要で、オンラインでの更新が可能です。分散システムを完全に隠ぺいしたシングルシステム・イメージでアプリケーションを開発できます。システム管理とアプリケーション開発を完全に分離することができます。

アクセス権の設定が可能
ブロックチェーンの記録閲覧や、コントラクトの変更・呼び出し等に、ユーザ／グループ、コントラクト単位のアクセス権限を設定できます。

（2018年当社調べ）

要件	A製品	B製品	DNCWARE Blockchain
パブリック or プライベート	パブリック	プライベート/コンソーシアム	プライベート/コンソーシアム
ブロックチェーンに記録する範囲	すべて データ・トランザクション・スマートコントラクトなど	データのみ	すべて データ・トランザクション・スマートコントラクトなど
記録の開示範囲	全て開示	アクセス制御可能 Ledger単位で	アクセス制御可能 User/Contract単位で
スマートコントラクト言語	Solidity	Go他	JavaScript
合意形成アルゴリズム	PoW/PoS	Orderingベース	Ben'Or (耐ビザンチン故障性)
基盤としての仮想通貨	あり	なし	なし