高信頼で使いやすい企業向けブロックチェーン

Highly Reliable and Easy-to-Use Enterprise Blockchain

遠藤　浩太郎 ENDO Kotaro　　外山　春彦 TOYAMA Haruhiko

仮想通貨ビットコインを起源とするブロックチェーン技術は，スマートコントラクトの誕生によりその適用領域が大きく広がりつつあり，更に幅広い分野での活用が期待されている。

そこで東芝グループは，利用者がスマートコントラクトを自由に作成することができる企業向けのブロックチェーンサービスを開始した。ブロックチェーンの本質を強化しつつも，一般のビジネス用途に配慮したアクセス制御と管理権限など，パブリックブロックチェーンとは一味違う技術を独自に開発し，高信頼で使いやすいブロックチェーンをマネージドサービスとして提供している。

The areas of application of blockchain technology, which originated from the cryptocurrency Bitcoin, are expanding significantly with the birth of smart contracts. Blockchain technology is therefore expected to be used in a wider range of fields in the future.

In response to this trend, the Toshiba Group has launched DNCWARE Blockchain+ (hereafter abbreviated as BC+), a blockchain service for businesses that allows users to freely create and deploy smart contracts. While strengthening the essential elements of blockchains, we have developed our own technologies that are unavailable in public blockchains such as access control and management privileges designed for general business use. As a result, we are able to offer a highly reliable and easy-to-use blockchain as a managed service.

1. まえがき

ブロックチェーンの歴史はビットコインから始まる。銀行を必要としない仮想通貨がその起源である。

ビットコインは不特定多数のマイナー（採掘者）によって共同運営されており，特定の一企業に依存しない。これは非中央集権的と称され，ブロックチェーンの重要な特長の一つとされている。

ビットコインを送金するトランザクション（取り引き）は，インターネット上の複数のマイナーが運用するコンピューター（ノードとも呼ばれる）に記録される。このとき，トランザクションをひとまとめにしたブロックを，暗号技術を使ってチェーン状につないで記録することで，改ざんを困難にしている。このデータ構造が，ブロックチェーンの名前の由来である。

ビットコインの様々な改良版が世界中で試される中，スマートコントラクトが誕生した。スマートコントラクトはすなわち，ブロックチェーン上で実行されるコンピュータープログラムである。目的に合わせてプログラムされたスマートコントラクトは，ブロックチェーンを様々な用途で利用することを可能にする。その結果，適用領域が拡大してきた。

具体的には，資金調達の手法であるICO（Initial Coin Offering）や，デジタル資産の取り引き手法であるNFT（Non-Fungible Token）などが，スマートコントラクトとして実用化されている。これらは，DeFi（Decentralized Finance）やWeb3.0といった非中央集権的な構想につながっていった。

将来的には，更に幅広い分野へのブロックチェーン技術の展開が有望であると考えられており，産業構造そのものへ影響を与える可能性も指摘されている[(1)]。

東芝グループは，顧客のデジタルトランスフォーメーションを支援するために，今後ブロックチェーン技術が鍵になると考え，高信頼で使いやすい企業向けブロックチェーンDNCWARE Blockchain+（以下，BC+と略記）を独自に開発し，マネージドサービスとして提供を開始した。

2. BC+の特徴

2.1 スマートコントラクト

BC+は，利用者が自由にスマートコントラクトを作成できるブロックチェーンである。開発しようとするアプリケーションに合わせてスマートコントラクトをプログラムすることで，利用者のアイデアに沿ってブロックチェーンの用途が広がっていく。

BC+のコンセプト（**図1**）では，スマートコントラクトを開発する利用者側と，ブロックチェーンのノードを運用するサービス提供側とで，権限が明確に分離される。サービス

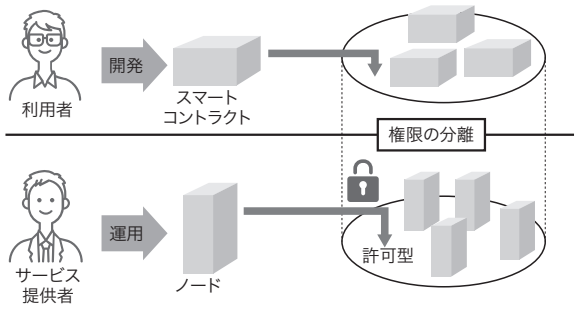

図1. BC＋のコンセプト

利用者がそれぞれにスマートコントラクトを作成することで，ブロックチェーンが成長していく。

Concept of BC+

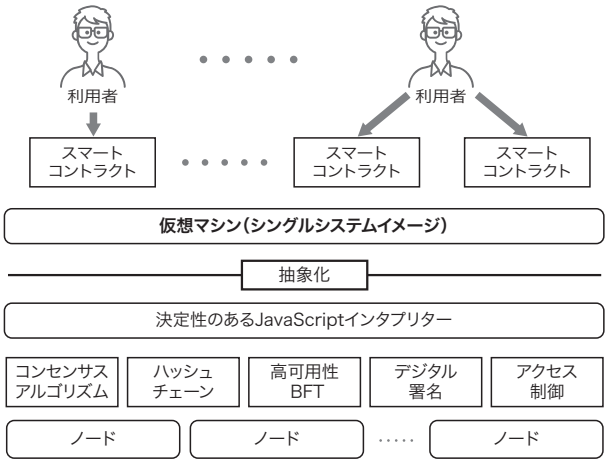

図2. シングルシステムイメージの構成

インタプリターのレイヤーで仮想マシンの抽象化を行い，複雑なブロックチェーンの仕組みを透過的にする技術を用いている。

Configuration of single system image

提供の側にはスマートコントラクトの開発に関与する権限は与えられておらず，一方，利用者は自由にスマートコントラクトの追加・変更をいつでもオンラインで行うことができる。

スマートコントラクトの記述言語は，JavaScriptである。よく使われているプログラミング言語を採用することで，言語習得の敷居を低くした。また，スマートコントラクトのプログラミングやデバッグなどの作業が一貫してできるツールを提供しており，利用者がWebブラウザーだけでスマートコントラクトを開発することも可能である。このツールは，ブロックチェーンの記録内容を参照する機能や，トランザクションを発行する機能なども備えている。

スマートコントラクトの実行モデルとして，シングルシステムイメージを実現した（**図2**）。スマートコントラクトは，ブロックチェーンに実装された仮想マシンの上で実行されると考えられる。その仮想マシンの動作は，ブロックチェーンを構成するノードの数に依存せず，利用者からは，あたかも1台の高信頼なコンピューターが動作するのと同じように見える。背後には，コンセンサスアルゴリズムや，ハッシュチェーン，デジタル署名などの仕組みがあるが，これらは透過的である。そのため，スマートコントラクトの開発にあたって，利用者はブロックチェーンの冗長化や保護の仕組みを意識しなくて済む。

このシングルシステムイメージの性質により，アプリケーションとノード運用の分離の境界が分かりやすくなり，スマートコントラクトの開発が容易になる。

2.2 許可型ブロックチェーン

BC+のブロックチェーンを構成するノードの運用は，特定の企業群によって行われる[注1]。このようなブロックチェーンは，一般に許可型ブロックチェーンと呼ばれる。許可型ブロックチェーンの特長の一つは，運用している企業が特定されているため，責任の所在が明確なことである。もう一つは，処理の完了（ファイナリティー）が高速にできるという点である。

なお，許可型ブロックチェーンの中には，ブロックチェーンを利用する際に，ノードの運用が前提となっているものもある。BC+はそれらとは異なり，ブロックチェーンのノードを利用者が用意しなくても，すぐに利用を始められる。

2.3 信頼性

ブロックチェーンは複数のノードで構成され，全てのノードが同じデータを記録するシステムとなっている。スマートコントラクトは全てのノードで実行される。障害のため一部のノードが停止した場合でも，その影響を受けずにスマートコントラクトの実行を継続できる。この構成のおかげで，高い可用性を持っている。

ノードの停止の原因には，故障のほかにも停電や定期的なメンテナンスなども含まれる。そのため，一部のノードが停止した場合でもサービスを継続できる高可用性は，多くのシステムに求められる重要な性質である。

もう一つの重要な性質として，ビザンチン障害耐性（BFT）がある。ビザンチン障害とは，故障による動作不良や，攻撃による誤動作，管理者が悪意を持って行う記録の改ざんなどの障害のことを指す。システム内の一部のノード内でビザンチン障害が発生しても，ほかの正常なノードがその影響を受けず，正しい動作を行う性質のことをBFTという。特にブロックチェーンの場合は，正常なノードの間で冗長化の

（注1） 執筆時点では，東芝グループだけによる運用であるが，今後コンソーシアムを形成して複数の企業や団体がノードを運用する形態にも対応していく予定である。

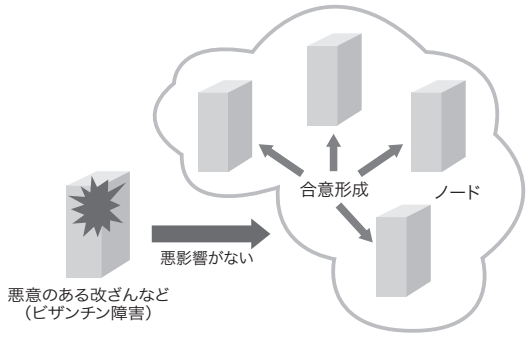

図3. BFTの概要

一部のノードの管理者が悪意を持って改ざんしても，ほかの正常なノードは悪影響を受けず，合意形成できる。

Outline of Byzantine fault tolerance

一貫性を維持できることも意味する（**図3**）。

ブロックチェーンにおけるBFTの最大の利点は，一部のノードで改ざんが行われても，ほかの正常なノードはその悪影響を受けないところにある。ノード運用のコンソーシアムを企業や組織の垣根を越えて広げていく際に，このBFTがあれば，参入を許容できる可能性が高くなる。

BC+は，高い可用性とBFTを持つようにあらゆる面から設計しており，合意形成に関わるノード数のうち20％未満（注2）のノード数のビザンチン障害に対して耐性がある。核となる技術は，当社が独自に開発したBFTを持つ合意アルゴリズム[2]である。これにより，BC+はコンソーシアムでの運用に適したブロックチェーンとなっている。

ところで，このような高信頼化技術はブロックチェーンに限らず，ミッションクリティカルなクラスターシステムに従前から適用されてきた技術である。東芝グループは，クラスター制御の根幹となる合意アルゴリズムを20年にわたり独自に研究開発し，製品に適用してきた。BC+に今回適用した合意アルゴリズムも，その長年の研究成果の一つである。

2.4 トラストレス

ビットコインのように，不特定多数のノードによって運営され，ノード運用への参加が誰でも可能なブロックチェーンは，一般にパブリックブロックチェーンと呼ばれる。このような運営形態が持続可能であることは，にわかには信じがたいが，事実がそれを証明している。成功の鍵はプルーフオブワークと呼ばれる巧妙な仕掛けにあるが，その背景の一つにトラストレスという考え方がある。文字どおりの意味は“信頼が必要ない”である。ブロックチェーンを前提に補足すると，“暗号技術を使って正しさを検証できる仕組みが備わっており，信頼を前提にしなくても，その記録が改ざんされていないことを証明できること”という解釈になる。

つまり，ビットコインの匿名のノード運用者を信頼することはできないが，そのノードの正しさは暗号技術を使って検証すれば証明できるので，信頼はそもそも必要ないということである。標語的には，“Don’t Trust，Verify.”という。

BC+では，トラストレスがブロックチェーンの本質であると考え，暗号技術だけを使って記録の正しさを利用者が検証できる設計にしている。また，ノード運用者の数が少ない場合の検証可能性の課題について，独自の特許技術[3]を使った対策をしている。

これにより，管理者が特定されているという許可型ブロックチェーンの特徴に加えて，その管理者が信頼できない状況でも，ブロックチェーン自体に改ざん検出の仕組みが備わっていることになる。

2.5 アクセス制御と管理権限

パブリックブロックチェーンでは，記録された内容は全世界に公開される。またデプロイしたスマートコントラクトは作成者の手を離れ，変更することも，停止することもできない。このような仕様は，究極の非中央集権を体現するもので，正しく理想的である。

しかし，この正しい姿が，一般のビジネス用途には適さないと考えられる場面は多い。例えば，企業間で取り引きした価格を第三者に見られたくないし，スマートコントラクトのバグを直す責任が誰かにある，と考えるのが普通である。ビジネスの常識は，究極の非中央集権とは相性が悪い。

そこでBC+では，ブロックチェーンの使いやすさを優先し，アクセス制御と管理権限の機能を実装した。

アクセス制御は，記録の内容を参照できる利用者を制限する。また，アクセス制御はスマートコントラクトごとに設定できる。

管理権限は，スマートコントラクトの変更や削除，そのほかの設定変更などを利用者に許可する。また，管理権限はドメインと呼ばれる枠内に効力がある。利用者は，利用開始時に自身だけが管理権限を持つドメインを取得し，このドメイン内にスマートコントラクトを作成していく。

アクセス制御や管理権限自体の設定変更も，管理権限によって利用者自身で行うことができる。つまり，これらの機能は，利用者に向けた機能として完結しており，シングルシステムイメージの上で動作し，ノードの管理者はこれらの機能に一切関与しない。

また，トラストレスを損なわないように注意深く設計されている。そのポイントは二つある。

（注2） 典型的な設定の場合。ほかに，高可用性を優先した設定や，逆にBFTを優先した設定が可能であり，その設定によってこの値は変化する。

(1) 利用者がアクセス制御のため記録内容を参照できない場合でも，ブロックチェーンの検証に必要となる，記録のハッシュ値は必ず参照できる。

(2) 管理権限による変更を行うとき，誰がどのような変更を行ったのか，その変更内容は全てブロックチェーンに記録される。

なお，この機能を使って，ドメイン内を究極の非中央集権の状態にすることもできる。そのためには，アクセス制御を全公開に設定した後，管理権限を設定変更して，誰も管理権限を持っていない状態にする。

3. サービス化と事業展開

世の中のデジタルトランスフォーメーションが進展していく中で，今後ブロックチェーン技術が鍵になると考え，利用者の意向に沿って柔軟に適用範囲を広げることができる，企業向けのブロックチェーンサービスを提供開始した。

利用者が自由にプログラムできるスマートコントラクトや，ノード運用とアプリケーション開発を明確に分離するシングルシステムイメージ，ミッションクリティカルな要求にも耐えられる高可用性，ノード運用のコンソーシアムの柔軟性を高めるBFT，非中央集権的な視点での安心をもたらすトラストレス，一般のビジネス用途に配慮したアクセス制御と管理権限などの技術を独自に開発し，同サービスに適用した。

このブロックチェーンサービスを利用して，Toshiba OPEN INNOVATION PROGRAM 2021の参加企業2社[4]，同2022の参加企業1社[5]と協業し，それぞれのアプリケーションの社会実装を進めている。ほかにも，顧客の企業や団体と連携した実証実験を行っている。

4. あとがき

ブロックチェーンの社会実装は，まだ始まったばかりであり，今後の発展の余地は大きい。今後もタイムリーな技術開発を行い，より良いサービスを提供していく。

文　献

(1) 経済産業省 商務情報政策局 情報経済課．平成２７年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書概要資料．2016，11p．<https://www.meti.go.jp/main/infographic/pdf/block_c.pdf>，（参照 2023-02-02）．

(2) 東芝．遠藤浩太郎．情報処理システム，サーバ装置，情報処理方法およびプログラム．特許第6158425号．2017-07-05．

(3) 東芝．遠藤浩太郎．改ざん検出システム及び改ざん検出方法．特許第6989694号．2022-01-05．

(4) 東芝．“「Toshiba OPEN INNOVATION PROGRAM 2021」参加企業8社と協業検討を開始し，プログラムが本格スタート”．ニュース．<https://www.global.toshiba/jp/news/corporate/2021/07/news-20210719-01.html>，（参照 2023-02-02）．

(5) 東芝．“「Toshiba OPEN INNOVATION PROGRAM 2022」参加企業9社と協業検討を開始”．ニュース．<https://www.global.toshiba/jp/news/corporate/2022/08/news-20220809-01.html>，（参照 2023-02-02）．

遠藤　浩太郎　ENDO Kotaro
デジタルイノベーションテクノロジーセンター 技術開発室
コアテクノロジー開発部
Core Technology Development Dept.

外山　春彦　TOYAMA Haruhiko
東芝デジタルソリューションズ（株）
デジタルエンジニアリングセンター マネージドサービス推進部
Toshiba Digital Solutions Corp.