次世代ICTを切り拓く ブロックチェーン技術

Blockchain Technology for Next Generation ICT

● 小暮　淳　　● 鎌倉　健　　● 島　常和　　● 久保竹清

あらまし

ブロックチェーン技術とは，中央集権機構を持つことなく，改ざん耐性，高可用性，透明性などを併せ持つ分散データ管理を低コストで実現する技術であり，次世代ICTを切り拓くブレークスルーとして期待されている。元々は，仮想通貨であるビットコインを実現するために考案された技術であるが，より広い金融分野，更には流通や，シェアリングエコノミーなど，様々な分野への応用が期待されている。一方で，応用範囲を広げるためには，データのプライバシー保護や処理性能向上などの技術的課題があるため，富士通研究所ではそれらを解決するための研究開発を行っている。

本稿では，まずブロックチェーン技術の概要および応用事例を紹介し，次にビジネスに適用する際の課題を解決する秘匿制御技術について解説する。最後に，富士通のブロックチェーン製品化・サービス化への取り組みと，その一環で行っているOSS（Open Source Software）プロジェクト活動について述べる。

Abstract

Blockchain technology, a low-cost decentralized distributed data management system featuring tamper resistance, high availability, and transparency, is a breakthrough technology that will lead to the next generation of information and communications technology (ICT). Originally devised to support the Bitcoin digital currency, it is expected to be applied to a broad range of financial applications as well as in various other sectors such as distribution and sharing economies. This broader application requires that several technical challenges including data privacy protection and better processing performance be addressed, and Fujitsu Laboratories Ltd. is working on several relevant R&D projects. This paper introduces blockchain technology and example applications, describes a technology for achieving security in a business context, and examines Fujitsu's efforts in commercializing this technology and an accompanying service as well as the open source software (OSS) project.

ま え が き

ブロックチェーンは，電子通貨であるビットコインを実現するために導入された技術の名称である。従来の電子通貨は，ある中央集権機構が電子データに価値を与えていたため，その機構の力の及ぶ範囲でしか流通できなかった。一方，ビットコインでは，中央集権機構を持たずに電子データを分散管理している。それにもかかわらず，電子データの価値を整合性の取れた形で，誰もが共通に認めることができる仕組みを導入することにより，世界で流通する初めての電子通貨を実現した。この画期的な仕組みの基となるのが，ブロックチェーン技術である。

なお，2014年2月に現金とビットコインを交換する電子通貨取引所であるマウントゴックス社が預り金を消失するという事件が起こったが，そのこととビットコインやブロックチェーンの信頼性とは無関係である。これは，両替所が運転資金を強奪されて破産しても，扱う通貨そのものの信頼性には影響しないことと同様である。

本稿では，このように社会的にも注目されているブロックチェーン技術について解説する。

ブロックチェーン技術の概要

まず，ビットコインにおけるブロックチェーンの仕組みを説明する。ビットコインでは，通常の金融取引における銀行口座に当たる概念をアドレスと呼ぶ。ビットコインの取引（トランザクション）は，入力となるアドレスとコインの量および出力となるアドレスとコインの量から成る。入力アドレスの所有者がトランザクションに電子署名を施すことにより，そのトランザクションがコインの持ち主が意図したものであることを保証する。

トランザクションは，ビットコインのピアツーピア（P2P）ネットワークを通じてブロードキャストされるが，悪意のある者の二重使用を防ぐために，全てのトランザクションを記録し，その正当性を皆で検証するという方針を採っている。この方針のもとで，10分ごとに正当なトランザクションのみを集めたデータセットをブロックと呼び，ブロックを時系列につないだものがブロックチェーンである。

このブロックの管理を第三者が行うインセンティブを与えるために，新しいブロックを最初に生成した人にビットコインが与えられるというルールが設けられている。ブロック生成競争を現実的なものにするために，ブロックのハッシュ値は，あるしきい値以下でなければならないという条件が課されている。そしてブロックの中のナンスと呼ばれる領域に乱数を振ることにより，10分ごとのハッシュ値計算競争が現実的にバランスの取れたものとなっている。また，ハッシュ値は次のブロックに取り込まれるため，過去のデータを変更すると，そこから先のブロックを全て再計算しなければ整合が取れない。このため，ブロックチェーンの改ざんは事実上不可能である（**図-1**）。更に，ビットコインのP2Pネットワークに参加する全てのノードが一意のブロックチェーンを共有して保持できるため，高可用性を同時に実現している。

このように，ビットコインのトランザクションはその時々ではばらばらに管理されているにもかかわらず，最終的には全体として整合性が取れた一意のブロックチェーンに収束し，改ざん耐性と高可用性を持つ情報（取引記録台帳）を共有できるシステムが実現されている。

図-1　ブロックチェーンの構造

ブロックチェーン技術を活用した取り組み

ビットコインのブロックチェーンは，ビットコイントランザクションのみをデータとして扱っているが，上述した原理によれば様々な種類のデータも同様な扱いが可能である。情報共有システムに対してブロックチェーンを適用する試みの事例として，みずほ銀行様と共同で行った証券クロスボーダー取引における実証実験を以下に紹介する。

証券クロスボーダー取引では，取引プロセスが複雑であるため，約定から決済までに通常3日間を要する。これは，約定から決済までの各プロセスにおいて，決済指図と約定内容との確認作業に多くの時間を取られるためである。昨今，価格変動などのリスクを避けるために，こうした取引プロセス期間の短縮が望まれている。実際，これまでにも集中管理方式のデータ共有により，プロセス期間を短縮する試みが検討されてきた。しかし，システムの運用管理コストが大きくなるなどの課題があり実現できていなかった。

みずほ銀行様との共同実証実験では，ブロックチェーンのOpen Assets Protocolを応用し，約定情報をブロックチェーンに記録するシステムを構築した（**図-2**）。このシステムにより，クロスボーダー取引に関わる全てのプレーヤーが改ざん不能となった約定情報を短時間で共有できることが確認され，結果として決済業務を3日間から即日に短縮できる可能性があることが明らかになった。

ブロックチェーン技術の適用分野の広がり

金融分野への適用から始まったブロックチェーン技術であるが，その適用先は金融分野にとどまらず，流通，サプライチェーン，公文書管理，シェアリングエコノミー，ヘルスケア，IoT（Internet of Things）など，様々な分野や領域が検討されている。また，適用分野の広がりに呼応するように，本技術自体も進化している。ビットコインだけではなく，より汎用的な価値，あるいは権利などの情報を扱うことや，あらかじめ定めておいた条件で自動的に契約が実行できる機構（スマートコントラクト）を持った様々なブロックチェーンが登場してきている。その例として，The Linux Foundationが設立し

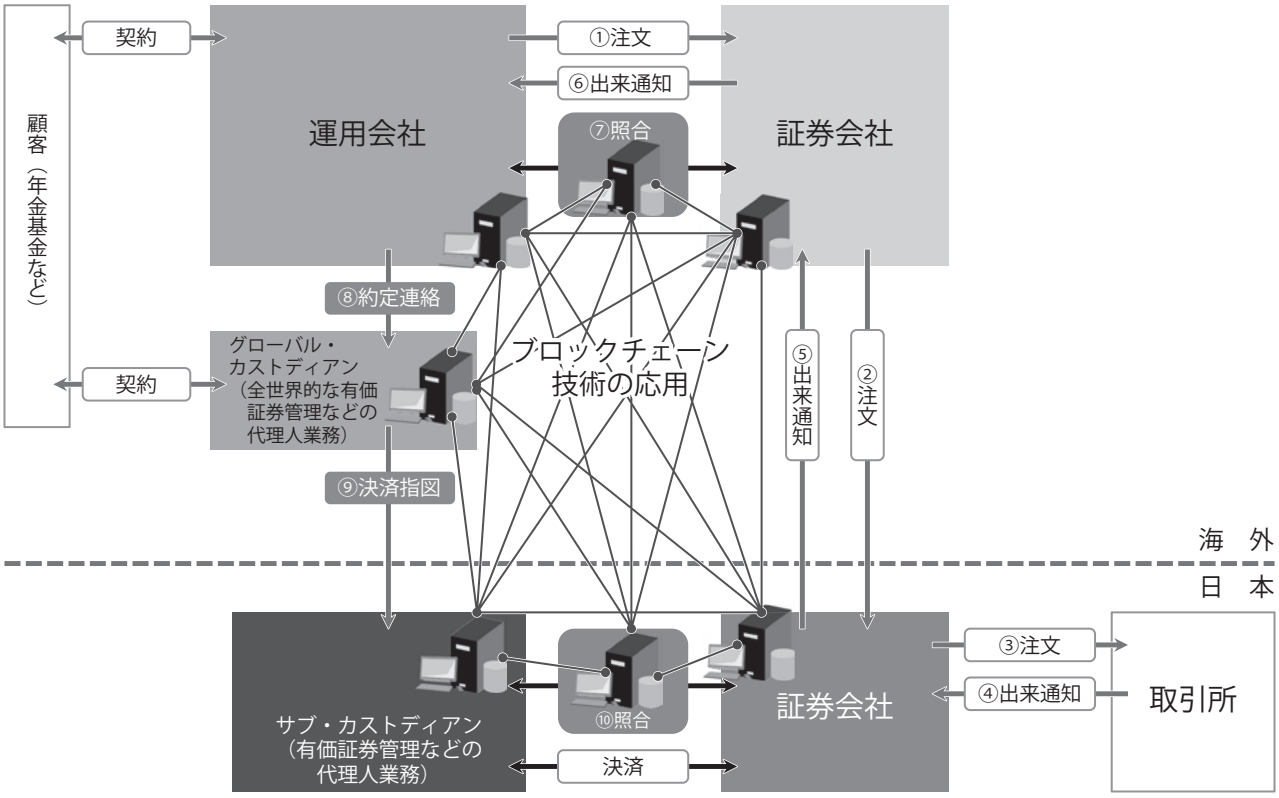

図-2　新たなクロスボーダー取引の決済フロー

たHyperledger Projectの一つであるHyperledger Fabric framework[1] やEthereum[2] などが挙げられる。

ここでは，金融分野以外の事例として，サプライチェーンへの本技術の適用を紹介する。例えば，原材料納入業者，製品加工業者，流通業者などの複数の組織でそれぞれ独立して管理されているデータ（取引記録，加工履歴，輸送履歴など）を，ブロックチェーンを使って統合する試みが検討されている。

期待される効果としては，原材料から小売までのサプライチェーンをトレース可能とすることで，需要に応じた効率的な製造や，効率的なリコールへの対処が可能になる。またIoTの観点では，スマートコントラクトを活用することで，製品加工業者の加工機械が加工数量に応じて原材料納入業者に原材料を自動発注し，管理コストを低減するといった使い方も可能である。

ブロックチェーン技術の課題

筆者らのこれまでの取り組みから，ブロックチェーン技術の課題としては，安全に使うためのセキュリティ機能の向上や，処理速度の向上などが挙げられる。

（1）セキュリティ機能の向上

ブロックチェーンは，取引情報を全てのネットワーク参加者で共有し，それぞれの参加者が取引情報に不正がないかを検証して取引情報の完全性を保証することを特徴とする。このため，ブロックチェーンを使用して行われた取引は，取引の当事者以外も参照できる。しかし実際には，取引の当事者以外にはその情報を公開できないケースがあるため，ブロックチェーンを使用して行われた取引の秘匿性をどのように確保するかという点が大きな課題である。

（2）処理速度の向上

ブロックチェーンを利用したシステムでは，従来型のシステムと比較すると，ネットワーク参加者間で取引を検証するため，処理速度が劣る。したがって，大量のトランザクションを扱うビジネス分野においては，処理速度の向上が課題である。

次章以降では，これらの課題のうち，セキュリティ機能の向上について論じる。

ブロックチェーン技術のビジネス適用に向けて

前述したようにブロックチェーンでは，データをオープンにしてネットワークを構成するノードが等しく検証可能な仕組みによりデータの完全性を保証する。しかし，これと引き換えに，ブロックチェーンに登録した全てのデータが同一ネットワークに参加している企業に公開されてしまう。

これに向けた対策の一つとして，ブロックチェーン上の情報を特定の関係者のみに限定して公開するアプローチが考えられる。限定公開するための秘匿化方法として暗号化が考えられるが，その場合，関係者が鍵の情報を共有する必要がある。容易に変更・削除ができないブロックチェーンの特徴に期待して情報を格納した場合，万一鍵の紛失や漏えいがあると，関係者はブロックチェーン上の情報を復号できなくなったり，暗号化して格納した情報が永遠に復号されるリスクにさらされたりしてしまう。

開発した秘匿化システム

今回，鍵の情報を安全に保存できる仕組みとして，秘密分散法を用いた鍵共有を実現した。秘密分散法は，鍵を複数の断片に分割し，分散した断片のうち一定数以上が集まると元の鍵を復元するための情報量が十分になるようにする。すなわち，全ての断片がそろわなくとも分割前の鍵を復元でき，また一定数未満の断片では復元できない。これにより，鍵の紛失や漏えいに対する安全性が向上する。更には，この方法を応用すると，複数の承認を要する手続きも実現できる。

今回試作したシステムの模式図を**図-3**に示す。ブロックチェーンには文書が格納され，文書の一部は当事者のみが閲覧できるように公開鍵暗号方式で秘匿されている。閲覧には暗号化で使用した公開鍵に対応する秘密鍵が必要であるが，そのまま共有せず秘密分散法を応用して安全性を向上させた。

今回は鍵を三つに分割し，当事者A，当事者B，文書作成者がそれぞれ保持し，三つのうちの二つが集まると元の秘密鍵が復元されるように設定した。したがって，当事者Aと当事者Bが協力することで秘匿した文書を閲覧できる。

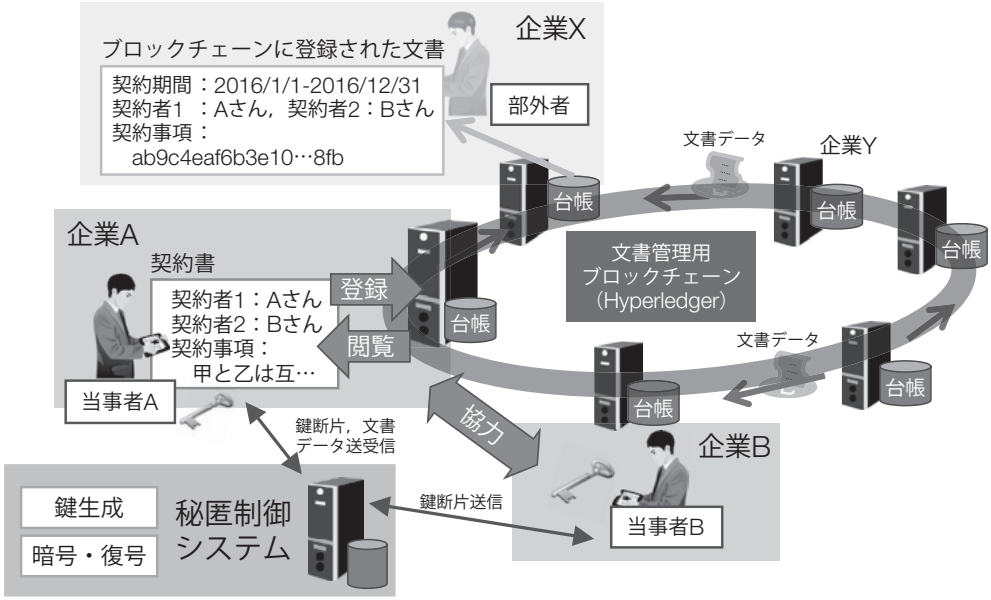

図-3　試作した文書秘匿化システム

鍵の生成や秘匿文章の復元は図-3の秘匿制御システム内で実施しており，そのアクセスにはWebインターフェースを利用している。このため，秘匿制御システムと各当事者が鍵の断片をこのシステムに渡す部分に関して，以下の安全性対策を施した。

・鍵の断片を保有する当事者の公開鍵で暗号化
・鍵の断片を復号する際，当事者がPIN（Personal Identification Number）コードを入力
・Webアプリケーション（復元された情報を含む）は，SSL（Secure Sockets Layer）経由でブラウザに表示
・端末で復号した鍵の断片をDH（Diffie-Hellman）鍵共有プロトコルを用いて秘匿制御システムに送信

文書を閲覧したい当事者が別の企業であると想定し，離れたオフィスでも作業できるように，Webブラウザを通じて秘匿文書が閲覧できるようにした。試作システムにアクセスすると，最初にブロックチェーンに格納された文書の一覧が表示される。当事者Aが秘匿された文書を選択し，自身が保有する鍵の断片①とPINコードを入力すると，鍵の断片①とブロックチェーンから取得した秘匿化された文章が秘匿制御システムに送信され，当事者Bに通知されるようになっている。通知を受けた当事者Bは，当事者Aが閲覧しようとしている文書を確認し，問題なければ自身が保有する鍵の断片②を指定する。鍵の断片②が秘匿制御システムに送信されると，秘匿制御システム内に十分な鍵の断片がそろう。こうして秘匿化文書を復号でき，当事者Aのブラウザの画面に文書が表示される。

試作した秘匿制御システムは，秘密分散法の原理に基づき，鍵の断片の一部（今回の場合は三つのうちの二つ）から元の鍵を復元している。この原理を応用すると，例えば鍵が保存された端末を紛失した場合に，上司などほかの複数の協力者によって鍵を復元するといったシーンに適用できる。更に，鍵の断片が取得できたことを申請に対する承認に見立てることで，複数の承認が必要なワークフローを実現することも可能である。

また，鍵の紛失時の被害を軽減する別の技術として，鍵の用途を限定するポリシーを鍵にリンクさせる技術も検討している。トランザクション署名鍵の用途をあらかじめポリシーとしてファイルなどに記述し，署名鍵に対応する検証鍵とポリシーとをシステムレベルでリンクさせておく。トランザクションをブロックチェーンに登録する際，トランザクションの検証鍵にリンクされたポリシーを確認し，トランザクションの内容がポリシーに反する場合には，ブロックチェーンに登録しない。この仕組みにより，署名鍵をポリシー以外の用途で使おうとしても，システムレベルでトランザ

クションを無効にできる。この技術により，送金先を特定の宛先のみに限定したり，送金金額の上限などを設定したりでき，紛失時の被害を軽減できる。

コミュニティへの参画

ブロックチェーン技術の効果が最大限に発揮されるためには，様々な新しいビジネスネットワークが創られ，それらが相互につながり，ビジネスネットワークが拡大していくことが必要である。この実現には，デファクトスタンダードになり得る基盤が必要であり，それにはOSS（Open Source Software）の活用が適していると考えている。

富士通は，The Linux Foundationのコラボレーションプロジェクトとして発足したHyperledgerに創設プレミアメンバーとして参画している。Hyperledger は，産業間共通のブロックチェーン技術推進のために設立されたOSSの共同開発プロジェクトである。米国富士通研究所（Fujitsu Laboratories of America）を窓口として，日本，ヨーロッパ，オーストラリアなど，世界中の富士通グループ各社がこのプロジェクトに関わっており，本プロジェクトを牽引していく。

富士通のアーキテクチャーコンセプト

富士通は，2016年10月にブロックチェーンのアーキテクチャーコンセプト「FMAB」を発表した[3]。

FMABは，ブロックチェーンそのものであるデータ管理レイヤーとビジネスに適用するために必要となるビジネス機能レイヤーに分割し，それぞれを進化させて，シームレスに連携することで，ブロックチェーンを使いやすい形でエンタープライズ領域に適用させていくコンセプトである。データ管理レイヤーには前述したHyperledger Fabric frameworkを搭載し，ビジネス機能にはデータのアクセスコントロールを行うためのデータ管理機能や，コンソーシアム型を容易に構築・運用できる参加メンバー管理機能を搭載している。これらの機能により，ブロックチェーン技術で課題とされてきたプライバシー問題の解決や，コンソーシアム参加者への信頼性向上が可能になる。

む　す　び

本稿では，ブロックチェーン技術をビジネスに適用する際の課題に対応する秘匿制御技術，および富士通のブロックチェーン製品化・サービス化への取り組みについて，OSSプロジェクトへの活動事例を交えて紹介した。

ブロックチェーン技術を適用したシステムは，従来の中央集権機構を持つデータ管理システムと発想が異なり，分散管理されているにもかかわらず整合性が取れた一意の台帳に収束するという特長を持つ。このため，改ざん耐性と高可用性を持つ情報共有システムを低コストに実現する，次世代ICTを切り拓くブレークスルー技術として期待されている。この技術を幅広くビジネスに活用すべく，今後も様々な要素技術の開発と実証実験を重ね，適用範囲を拡大していく。

参考文献

（1）The Linux Foundation：Hyperledger Project. https://www.hyperledger.org/

（2）Ethereum Project. https://www.ethereum.org/

（3）富士通：金融ソリューション ブロックチェーンの取り組み. http://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/

著者紹介

小暮　淳（こぐれ　じゅん）
ライフイノベーション研究所
ブロックチェーン応用研究に従事。

鎌倉　健（かまくら　けん）
セキュリティ研究所
データセキュリティ関連の研究に従事。

島　常和（しま　つねかず）
ライフイノベーション研究所
ブロックチェーン応用研究に従事。

久保竹清（くぼ　たけきよ）
金融システム事業本部
デジタルビジネス事業部
ブロックチェーンサービス開発に従事。