ブロックチェーン技術の動向

星 暁雄 ●ITジャーナリスト

プライベートブロックチェーンのエンタープライズシステムへの実証実験が進み、実システムへの適用事例も登場。パブリックブロックチェーンではDAppsが急増中。今後は2nd Layerやクロスチェーンの進展に期待。

ブロックチェーン技術は大きく2つに分かれる。1つは仮想通貨のインフラであるパブリックブロックチェーン、もう1つは情報システムのデータ基盤として設計開発されたプライベートブロックチェーンである。後者には、より広い概念である分散型台帳技術（Distributed Ledger Technology、DLT）の用語を使う場合もある。両者の性格は大きく異なる。まずはプライベートブロックチェーン技術に関する話題を見ていくことにしたい。

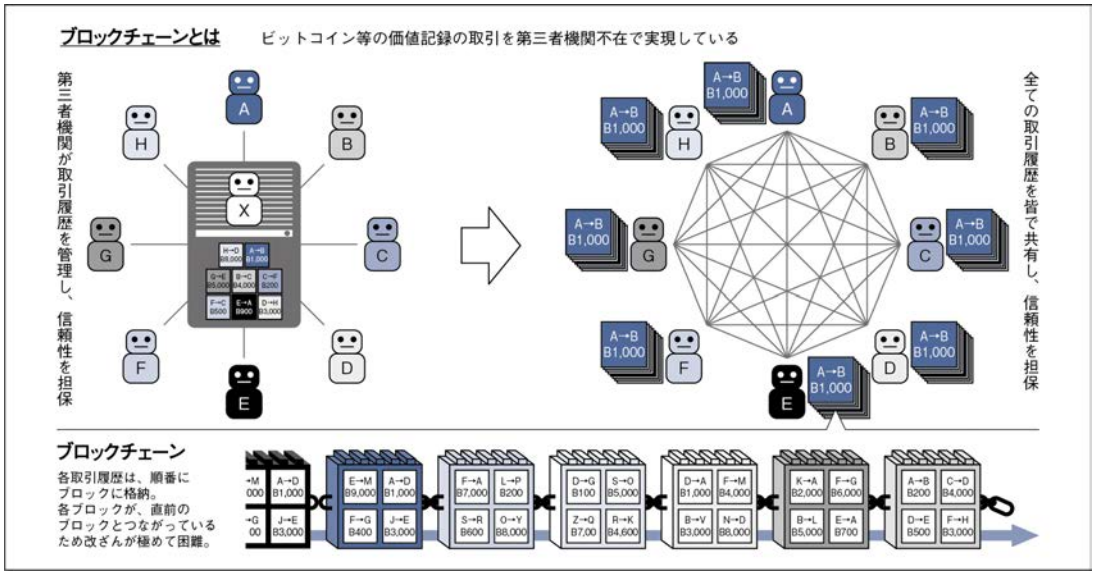
■プライベートブロックチェーン技術への取り組みが進む

プライベートブロックチェーンは、情報システムの一部として管理運用されるブロックチェーンである。この分野を狙い、IBMが開発してLinux Foundationに寄贈したHyperledger Fabric、金融分野を対象とするベンチャー企業R3が開発したCorda（これは分散型台帳技術と位置づけられる）、J.P. Morganが開発したQuorum（Enterprise Ethereum Alliance、EEAのコンセプトに基づく）などのオープンソースソフトウェアプロダクトが登場している。また日本のベンチャー企業が開発したプライベートブロックチェーン技術として、テックビューロのmijin、ビットフライヤーのMiyabiなどがある（両者とも記事執筆時点ではオープンソースではない）。

2017年は、プライベートブロックチェーン技術のエンタープライズシステムへの応用がじわじわと進行した年となった。銀行や証券取引所などでの実証実験による知見の蓄積が進み、ブロックチェーン技術を採用したシステムが実稼働にこぎつけた事例も登場した。

ブロックチェーン／分散型台帳技術（以下、ブロックチェーン技術）を情報システムに適用する場合のイノベーションは、「第三者機関への信用を必要とせず、複数の人間／組織が1つの共有台帳を信用できること」と要約できる（資料2-2-1）。会社どうしが取引をする場合、システムがどれだけ進化していたとしても組織の境界で伝票を確認する手作業（リコンサイル）が発生する。

資料2-2-1　ブロックチェーン技術の概念図



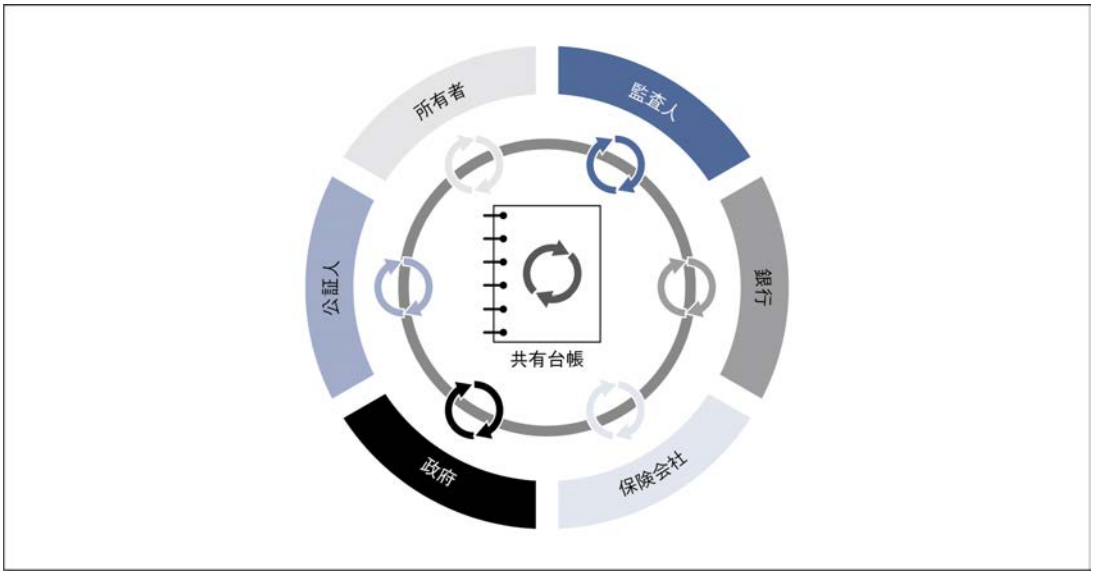
出典：経済産業省「ブロックチェーン技術を利用したサービスに関する国内外動向調査」（2016年4月）

このような手間を回避して業務を効率化するには、従来は信用できる中立的な第三者機関が運用する情報システムを使っていた。例えば銀行間送金を手がける全銀ネットが、このような第三者機関に相当する。ブロックチェーン技術の登場で、この「信用できる中立的な第三者機関」の役割をソフトウェアだけで実現でき、複数の会社にまたがる業務を大幅に効率化できる可能性が出てきている（資料2-2-2）。この期待がプライベートブロックチェーン技術への期待に結びついている。なお、これとは別にブロックチェーン技術を使うことで可用性が高いシステムを従来手法より安価に構築できるとの期待もある。

このような期待のもと、ブロックチェーン技術を銀行間送金、証券取引所、サプライチェーン管理、貿易金融、学歴情報の管理、シェアリングサービスの本人確認など、幅広い分野に応用する取り組みが進んでいる。さらには、市中銀行発行のデジタル通貨（例えば三菱東京UFJ銀行は「MUFGコイン」の実証実験を進めている）、国の中央銀行発行のデジタル通貨のような社会的影響が大きな応用についても真剣な検討が進んでいる段階である。

多くの取り組みは着実な進め方をしており、爆発的な普及という印象はまだない。ブロックチェーンとは「信用できるデータ基盤」というシステムの根幹に係わる技術なので、その活用も新規システムのインフラに採用するかどうかの検討から始まることになり、実利用の事例が登場するまでには長い準備期間が必要となる。2017年はブロックチェーン技術を実利用するための準備期間だったと位置づけられる可能性が高いのではないだろうか。

資料2-2-2　共有台帳による業務効率化の概念図



出典：IBM「ブロックチェーンが引き起こす劇的な変革のシナリオ：基調編〜企業・エコシステム・経済の再考〜」

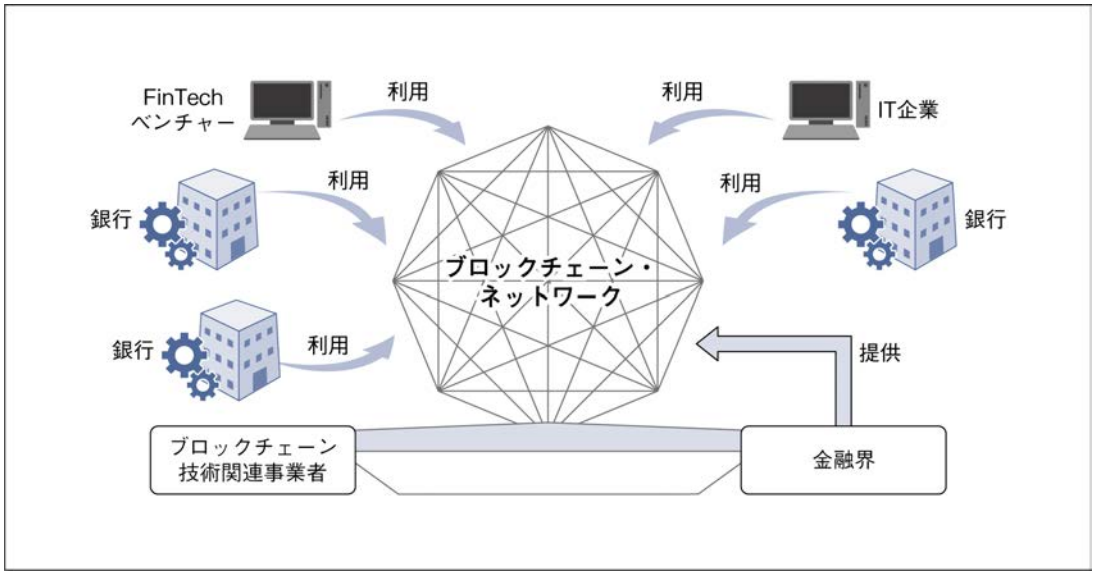
■ブロックチェーン活用の取り組みは地道に進む

ブロックチェーン技術への取り組みとして一例を挙げると、ウォールマートは、グローバルな食品サプライチェーン管理にブロックチェーン技術を適用する取り組みを進めている。金融分野以外での本格的ブロックチェーン活用として注目されている。同社が組んだITベンダーはIBMで、利用する技術としてHyperledger Fabricを活用する方向である。ブロックチェーン技術の特徴といえる、複数の当事者が信頼できる台帳を実現する特質を使った事例といえる。

日本国内の事例として、JPX（日本証券取引所グループ）は、2016年に実証実験として証券市場の基本的な機能を分散型台帳技術により実装したアプリケーションを開発している。2017年は「日本株取引のポストトレード業務」および「顧客確認業務」の2件のアイデアの検証に取り組んだ。

日本の銀行のほとんどが加入する全国銀行協会（全銀協）は、ブロックチェーン技術を決済・送金サービスや本人確認・取引時確認（KYC）、金融インフラの分野に適用する実証実験プラットフォームを立ち上げ、加入する銀行がさまざまな検証を進める環境を整えた（資料2-2-3）。この実証実験プラットフォームに選ばれたブロックチェーン技術はHyperledger FabricとMiyabiである。実システムに至るまでには今後長い準備期間が必要となるだろうが、金融機関がブロックチェーンを本格的に評価検討する動きを進めていることには注意しておきたい。

資料2-2-3　全国銀行協会（全銀協）が立ち上げた実証実験プラットフォームの概念図



出典：全銀協プレスリリース

日本ジビエ振興協会は、野生の鳥獣の食肉「ジビエ」の流通を追跡確認するトレーサビリティを実現するシステムをブロックチェーンを活用して構築し、2018年初頭から運用を開始する。テックビューロが開発したmijinを採用した。プライベートブロックチェーン搭載の実システム稼働の公表事例として日本で最初の事例となる。導入の理由として「開発工数と運用コストの削減」を挙げている。プライベートブロックチェーン技術では高い可用性を標準機能の範囲で実現できることが背景にある。また耐改ざん性があり監査可能であることも、トレーサビリティを実現するシステムとの相性がいいといえる。

■「ファイナリティ」をめぐりブロックチェーン技術は2つに割れる

金融分野へのブロックチェーン活用でよく目にする言葉が「ファイナリティ」である。もともとは決済の確定性を意味する用語なのだが、ブロックチェーン技術の文脈では、取引記録が覆る可能性がないという意味で使われる。

ビットコインやEthereum（イーサリアム）を筆頭とするパブリックブロックチェーンの合意形成アルゴリズムは「時間が経過すると共に取引記録が覆る確率が0に収束する」挙動を示す。このような確率的な挙動を許容することにより、数千ノードという超大規模なP2Pネットワークや、ノードの参加や脱退が自由という重要な特徴が得られているともいえる。ただし、確率的な挙動は金融分野に当てはめると「ファイナリティがない」と解釈されるので受け入れられないと考える人はまだ多い。

そこで、金融分野への適用を視野に入れたプライベートブロックチェーン技術の多くでは確定的な合意形成アルゴリズムを採用する。これらのアルゴリズムは、分散システム研究から生まれた分散合意形成アルゴリズムのPaxosやPBFT（Practical Byzantine Fault Tolerance）の延長にある。これらのアルゴリズムは動作が確定的となる半面で、ノード数増大に伴いプロトコルのオー

バヘッドが増大するのでノード数には上限があり、またノード数は既知でなければならず、ノードの参加/脱退は厳密に管理する必要がある。

このように、「ファイナリティの有無」とはブロックチェーン技術の設計思想にまでさかのぼる問題といえる。ファイナリティの追求で得られるもの、失うものがそれぞれ存在することには注意を払う必要があるだろう。

■IBM、Microsoftに加えてAmazon、Oracleがクラウド上のブロックチェーン環境を提供

2017年は、ITベンダーによるブロックチェーン技術への取り組みにも進展があった。

IBMは、同社が開発したブロックチェーン技術をLinux Foundationが推進する「Hyperledgerプロジェクト」にHyperledger Fabricとして寄贈し、オープンソースプロジェクトとして推進している。Hyperledger Fabricに対してはアクセンチュア、富士通、日立製作所、NEC、NTTデータなどシステム構築大手が賛同し、取り組みを進めている。クラウドサービスIBM Bluemix上では、Hyperledger Fabricを手軽に試せる環境を提供している。またIBMは、10月からメインフレームz Systemsの機能を活用してセキュリティをさらに強化したブロックチェーンのサービス「IBM Blockchain Platform」の提供を開始した。実稼働環境での利用を狙うサービスといえる。

MicrosoftのクラウドサービスAzureでは、R3 Corda、Quorum、Hyperledger Fabricなど複数のブロックチェーン技術および分散型台帳技術をクラウド環境で試せるサービスを提供している。

クラウド最大手のAmazonは従来はブロックチェーン技術に消極的と思われていたが、2017年12月になって「AWS Blockchain Partners Portal」を発表した。IntelのSawtooth、R3 Corda、Quorumなどを同社クラウド上で活用可能とし、それぞれの技術のソリューションパートナーとユーザー企業が協力しやすい環境を提供する。ただしサービスの説明ページにはIBMらが推進するHyperledger Fabricの記載はない。

Oracleは、8月にHyperledgerプロジェクトへの賛同を表明し、10月に「Oracle Blockchain Cloud Service」を発表した。記事執筆時点では近日開始予定となっている。

こうした一連の取り組みは、クラウドベンダーの顧客のエンタープライズシステム構築の現場で、ブロックチェーン技術を評価検討する需要が増えていることを反映している。ブロックチェーン技術をクラウドサービス上で手軽に評価できることは、開発者人口の増大、技術の普及に寄与するだろう。

■パブリックブロックチェーンは独自に進化

以下、パブリックブロックチェーンの動向を見ていく。パブリックブロックチェーンは特定の運用管理主体を持たないP2Pネットワークとして稼働することが大きな特徴である。仮想通貨の多くが独自のパブリックブロックチェーンを持っている。

ビットコインは今なお重要なパブリックブロックチェーンであり、新技術の開発、検討も活発に行われている。ビットコインは数千ノードという超大規模なP2Pネットワークに成長していて、9年間にわたりほぼ無停止で動き続けていることから、パブリックブロックチェーンとして最高水準の信用を得ているといえる。ただし、需要の高まりに伴い処理能力が仕様上の上限に達していることが課題である。2017年のビットコインは、課題となっていた性能向上（スケーリング）をきっかけにコミュニティの「分裂」騒動が話題

となった（詳細は本書第5部「仮想通貨の動向」の項目を参照）。今後は、新仕様SegWitの普及、Lightning Network技術の成熟と普及などが期待されている。

ビットコインに次ぐ規模の時価総額に成長した仮想通貨（オルトコイン）であるEthereumは、「ワールドコンピュータ」のコンセプトに基づくパブリックブロックチェーンを備えている。Ethereumはブロックチェーン上の価値移転を制御できる「コントラクト」と呼ぶプログラムを実行する機能を備える。これは条件分岐などプログラム特有の処理を適用したうえでの価値移転を記述、実行できるもので、平たくいえば「お金を扱う契約」をプログラムとして実現できる環境が登場したことになる。その意味で「スマートコントラクト」という名前でこの機能を呼ぶ場合も多い。

Ethereumのコントラクトを活用したアプリケーション（Decentralized Applications、DAppsと呼ぶ）の活用例は900種類以上が登場している。DAppsの例としては、予測市場、分散ストレージ、分散型取引所DEX（Decentralized Exchange）などがある。2017年にはEthereumブロックチェーンの上で「猫を飼う」ゲームである「CryptoKitties」が思わぬ人気を呼び、Ethereumが処理するトランザクションの20%に達したという"事件"も起きた。

Ethereumでは、処理性能を分散処理で高めるシェーディングや2nd Layer技術への取り組み、また大量の電力消費を伴うPoW（Proof of Work）から電力消費を抑えたPoS（Proof of Stake）への移行など、冒険的な取り組みを多数計画している。ビットコインが保守本流とすればEthereumは革新派との位置づけともいえる。

2017年にEthereumの技術を金融をはじめとするエンタープライズシステム分野に適用するEnterprise Ethereum Alliance（EEA）が発足し、日本からもKDDI、トランスコスモスらが参加している。EEAはエンタープライズシステム分野に向けた別仕様のEthereumである「Enterprise Ethereum」を構築し、パブリックブロックチェーンのEthereumとハイブリッドで機能させることを目指している。

■プライベートブロックチェーンとパブリックブロックチェーンの連携が次の目標

パブリックブロックチェーンとプライベートブロックチェーンのそれぞれのメリット、デメリット、適用範囲に関しては専門家の間でもなかなか意見が一致しない場合がある。両者をあえて比較するなら、不特定多数のマイナーが支えるパブリックブロックチェーンは対改ざん性という観点でより強靭で、また台帳の内容が広く公開されているという点で透明性がある。例えば難民支援のためのID発行というユースケースがあるが、これはパブリックブロックチェーンならではの活用法といえるだろう。

一方、プライベートブロックチェーンは、性能を追求でき、運用管理上の仕組みを作り込むことができ、情報プライバシーを保護しやすい特徴があるといえるだろう。ブロックチェーン技術はもともと可用性の高さ、対改ざん性や監査可能性、外部からの攻撃や内部不正にも強いという性質があり、情報システムのデータ管理基盤として有効に使える可能性がある。この分野の知見の蓄積を期待したい。

この両者に関係する重要な動きとして、パブリックブロックチェーンとプライベートブロックチェーンを相互に連携させた活用方法の議論、提案が始まっている。例えば、パブリックブロックチェーン上で定義された価値（例えば預かり金残高を示すトークン）をプライベートブロック

チェーンに移転したうえで高速に処理する使い方である。将来は、パブリックブロックチェーンとプライベートブロックチェーンの両方を活用するスタイルが普及していく可能性もあるだろう。

複数のブロックチェーンの連携（クロスチェーン）の分野でも、サイドチェーン、アトミックスワップ、ILP（Inter Ledger Protocol）のようにいくつかの試みが同時進行で進んでいる。要注目の分野といえる。今後は、パブリックブロックチェーンの信用と透明性、プライベートブロックチェーンの高速性と柔軟性、そして高速・高頻度の決済を可能とする2nd Layer技術、異種ブロックチェーンを連携させるクロスチェーン技術を組み合わせた新たな活用のスタイルが登場するのではないかと予想している。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2018年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp