ブロックチェーンによる企業間連携の実用化に向けた取り組み

鳥山 慎一　宮岸 聖高　並木 悠太　小出 俊夫

要 旨

ブロックチェーンは、サトシ・ナカモト氏により提唱されたBitcoinの基幹となる分散型台帳システムであり、現在もさまざまな団体や企業により研究開発が進められています。その利活用の可能性は今や仮想通貨だけにとどまらず、金融機関間の送金や証券取引、貿易取引などに広まっています。本稿では、ブロックチェーン技術を解説し、NECの取り組みと独自の技術を紹介します。

KeyWords
ブロックチェーン／データ構造／P2Pネットワーク／合意形成アルゴリズム／Hyperledger Fabric／サテライトチェーン

1. はじめに

2008年サトシ・ナカモト氏によりBitcoinに関する論文「Bitcoin: A Peer-to-Peer Electronic Cash System」が発表され、その翌年にBitcoinの運用が始まって以来、その基幹であるブロックチェーンは、中央管理者を持たずに分散してデータを保持し、データの消失や改ざんを発生させることなく仮想通貨の価値を支えてきました。FinTechにおいて大きな注目を集め、金融業界や政府関連を中心に、国内外を問わず活用に向けた実証実験が盛んに行われています。

2. ブロックチェーンとは

ブロックチェーンは、分散してデータを管理する仕組みです。参加者全員が同じデータを保持するため、一部の参加者のノード(システムを構成する1台のコンピュータ)で障害が発生してもそれ以外のノードで処理を継続することが可能であり、高い業務継続性を実現します。また、データは順次、前のデータとそのハッシュ値を用いて連結されているため、データの改ざんは非常に困難です[1)]。

2.1 ブロックチェーンの要素技術

ブロックチェーンは、データ構造(ハッシュ値により連結されたデータ・電子署名)とP2P(Peer-to-Peer)ネットワーク、合意形成アルゴリズム(複数のノードが同じ動作をするための仕組み)の要素技術を持ちます。

データは、ブロックと呼ばれる単位にまとめられます。ブロックは、前のブロックのハッシュ値を含めることで、ハッシュ値により連結された構造をとります(**図1**)。そうすることで仮にブロックのデータの改ざんが行われた場合、その改ざんしたブロック以降に生成されたすべてのブロックのハッシュ値も変更する必要があるため、チェーンが長くなればなるほど、データの改ざんは非常に困難になります。なお、データには電子署名を付与し、その正しさを保証します。

P2Pネットワークは、中央管理者に頼ることなく、参加するノードがそれぞれデータを保持し、他のノードに対し

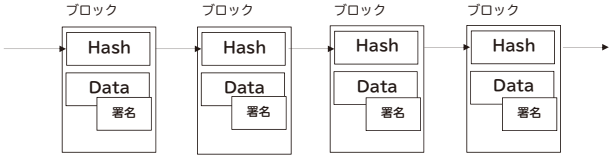


図1　ブロックチェーンのデータ構造

て対等の関係でデータの要求と提供を行います。

合意形成アルゴリズムは、それぞれのノードがデータを持つP2Pネットワーク上で、システムとして唯一の正しいデータを決定するために使用されます。Bitcoinのブロックチェーンでは、Proof of Work(PoW：仕事量を元に正当性を決める考え方)と呼ばれる方式が採用されています。

2.2 ブロックチェーンプラットフォーム紹介

現在、複数のブロックチェーンプラットフォームが存在しており、それぞれ特徴を持っています。ここでは、代表的なブロックチェーンプラットフォームとしてBitcoin、Ethereum、Hyperledger Fabricを紹介します。

Bitcoinは、ブロックチェーンにより銀行のような管理者に依存しない運用を実現した仮想通貨です。Bitcon誕生後、その基幹であるブロックチェーンを仮想通貨だけでなく、より汎用的に活用できるようなプラットフォームが開発されました。

Ethereumは、Vitalik Buterinが書き下ろしたホワイトペーパーを元に開発し、2015年7月にリリースされました[2)]。Bitcoinの仮想通貨に対する操作に相当する部分を、ユーザーが自由にプログラミングできるようにし(スマートコントラクトと呼ばれる)、ブロックチェーン上で任意のプログラムを実行可能にするプラットフォームです。なお、近々、エンタープライズ用途を想定したEnterprise Ethereum、がリリースされる予定です。Ethereumと比較してスケーラビリティとプライバシーの保護を強化したものになっています[3)]。

Hyperledger Fabricは、Ethereum同様、ブロックチェーン上で任意のプログラムを実行可能にするプラットフォームですが、エンタープライズ用途を想定し、BitcoinやEthereumと異なる合意形成アルゴリズムを採用しています。これはPBFT (Practical Byzantine Fault Tolerlance) と呼ばれるもので、一定の規模のネットワークにおけるProof of Work(PoW)などより高速な合意形成とファイナリティ(処理が覆らないものとして確定すること)を担保しています。現在、公開されているバージョンはv0.6ですが、近々にv1.0がリリースされる予定です。特徴は、スケーラビリティ(デフォルトで分散合意形成を使用)とセキュリティ(認証局によりユーザー証明書や匿名証明書の発行が可能)を強化したものになっています[4)]。

これらのプラットフォームは、それぞれの特徴からパブリック型、コンソーシアム型、プライベート型に大きく分類することができます。パブリック型では参加者は自由にネットワークに参加することができ、大規模なネットワークにも対応できる合意形成アルゴリズムが用いられます。コンソーシアム型やプライベート型は、名前のとおりコンソーシアムあるいは、ある組織に所属するメンバーのみがネットワークに参加可能としたもので、小規模な構成で効率よく動作する合意形成アルゴリズムが用いられるなどの違いがあります(**表**)。

表　ブロックチェーンプラットフォームの分類

分類	非許可型	許可型	
	パブリック型	コンソーシアム型	プライベート型
管理者	管理者なし	複数企業	1社(自社)
ノードの参加	自由	許可制	許可制
取引 (トランザクション)	自由	許可制	許可制
ブロックチェーンへのアクセス	自由	許可制	許可制
新規ブロック承認方法 (マイニング/合意形成)	Proof of work Proof of Stake	許可された参加者による承認 (BFT:Byzantine fault toleranceなど)	自己承認(BFTやレプリケーションなど)
代表的なサービス/プラットフォーム	Bitcoin, Ethereum,Altcoins, Rippleなど	Hyperledger Fabric, R3CEV, Orb, Erisなど	Mijin, MASDAQ Linqなど

3. ブロックチェーン技術に対するNECの取り組み

3.1 論文発表

NECでは、早期からブロックチェーンの研究に取り組んでおり、その成果は、著名論文誌(ACM TISSEC)や国際会議(ACM CCS)に採択され、Bitcion XTの公式実装に採用されています。更に、学会誌での記事の執筆などブロックチェーンの発展に向けた活動を行っています。

3.2 Hyperledgerプロジェクトへの参画

NECはブロックチェーンの実用化に向け、2015年12月に設立された Hyperledgerプロジェクト(**図2**)に参画しました[5)]。

3.3 IIIブロックチェーン研究会の設立

株式会社 日本総合研究所が主催する異業種連携によ

る事業コンソーシアム（Incubation & Innovation Initiative 「III」：トリプルアイ）では、NECが主体となり2016年4月に「III ブロックチェーン研究会」（**図3**）

2015年12月設立
主要会社
NEC，IBM，富士通，日立，NTTデータ，J.P. モルガン，SWIFT，ドイツ証券取引所など（現在100社が参加）
目標
- ブロックチェーンのフレームワーク共同開発、開発者育成を目指す協業プロジェクト。
- 共同開発することで一企業や業界では成し得ない速度と深度でブロックチェーン技術の導入には何が重要であり、現在何が欠落しているのかを見極め、対応するフレームワーク構築を目指す。

図2　Hyperledgerプロジェクトの概要

目的	ブロックチェーン技術を活用した新たな事業創出の貢献
活動内容	➢ NEC有識者レクチャーによる勉強会 ➢ ブロックチェーン利活用のディスカッション ➢ テスト環境での検証、及び、商用化に向けた課題などの考察結果の共有
ゴール	➢ ブロックチェーンの特性を理解し、効果の高いユースケースの整理 ➢ テスト環境を用いての特定ユースケースの検証を通じて、実運用における課題の洗い出し

図3　IIIブロックチェーン研究会の概要

を設立し、ブロックチェーン技術を活用した事業創出を検討しています[6]。

これらの取り組みを通して、NECはユースケースに適用する際のブロックチェーンの課題に対する解決を検討し、NEC独自のブロックチェーン技術を開発しました。

4. Hyperledger Fabricとサテライトチェーン

Hyperledger Fabricは、ノードの参加、ブロックチェーンへのアクセス、新規ブロック作成の承認を特定の者に限定して行うため、パブリック型のブロックチェーンに比べ、合意形成の時間を短縮できますが、その合意形成の時間はノード数に依存しているため、ノード数の増加に伴う処理速度の低下によって実運用に耐えられない可能性があります（スケーラビリティの制限）。また、現時点のバージョン（v0.6）では、データを秘匿化する機能が実装されていないため、複数の企業・団体・グループが参加する場合でのユースケースに適用が難しい可能性があります（プライバシーを保護できない）。

NEC独自のブロックチェーン技術であるサテライトチェーンは、複数のブロックチェーンネットワークを動的に作成し、互いに連結することで一つのブロックチェーンあたりのノード数の増加を抑止し、結果として処理速度（スループット）の低下を抑止可能とする技術です。特定のノードだけでネットワークを形成できるので関係者以外からのデータの閲覧を防止することができます。つまり、サテラ

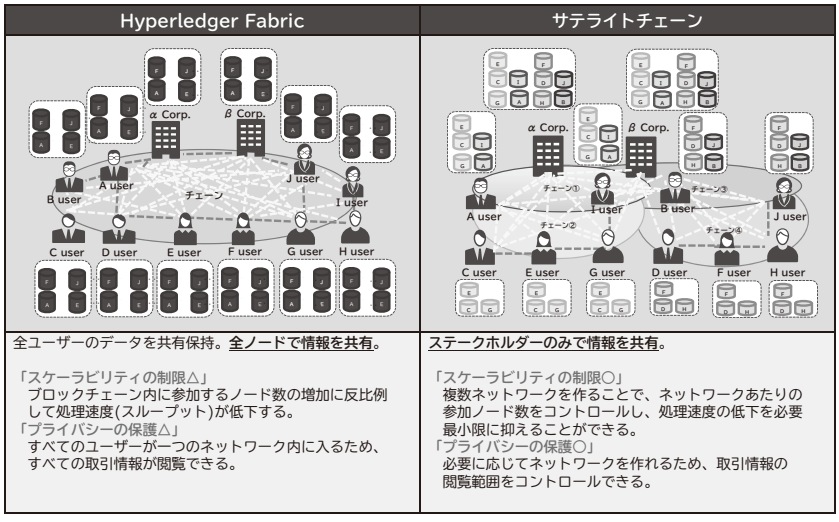


図4　Hyperledger Fabricとサテライトチェーンの違い

イトチェーンは、Hyperledger Fabricの「スケーラビリティの制限」と「プライバシーを保護できない」課題をそれぞれ解消できます（**図4**）。

サテライトチェーン技術を適用することでHyperledger Fabricに比べてより柔軟にユースケースに合わせたシステムを形成することができます。例えば、ブロックチェーンネットワーク数を調整することで、複数の企業・団体・グループが参加し、関係者内外でデータの秘匿化が必要となるコンソーシアム型と、一つの企業・団体・グループ内で用いられ、基本的にはデータの秘匿化が不要なプライベート型の、どちらのユースケースにも対応可能です。

5. これまで検討・適用したユースケース

経済産業省はブロックチェーンの活用に親和性のある5つの類似化されたユースケースを例示しています[7]。

（1）価値の流通・ポイント化プラットフォームのインフラ化
（2）権利証明行為の非中央集権化の実現
（3）遊休資産ゼロ・高効率シェアリングの実現
（4）オープン・高効率・高信頼なサプライチェーンの実現
（5）プロセス・取引の完全自動化・効率化の実現

これらのユースケースの共通点は「複数のステークホルダーが存在する業務」です。NECは、これまで行った「複数のステークホルダーが存在する業務」のブロックチェーン化に向けた提案と業務特性を考慮した実証実験を通じ、実現の可能性の確認、及びブロックチェーンを利用した場合のメリット・デメリットや課題・制約事項を整理しました。その結果、環境的な制約と技術的な観点から署名作成用の「鍵」をクライアント端末側に配置できなかったこと、合意形成アルゴリズムの問題などの課題が挙がりました。今後は課題解決に向け、金融機関が取り組む信託業務へのブロックチェーン技術の活用に向けた実証実験を支援するなど、ユースケースごとの設計方法の検討やブロックチェーンプラットフォームの研究開発を行っていきます[8]。また、これまで得られた知見を生かし、他のユースケースの適用も目指します。

6. むすび

ブロックチェーンは、今後もFinTechにおいて大きな注目を集めていくとともに、利活用に向けた更なる検討が行われることが予想されます。しかし、現時点でさまざまなユースケースに幅広く対応できるブロックチェーンプラットフォームが少ないことや、運用方法・開発標準などが未成熟なことから、実業務に適用可能になるのは早くて5年先とも言われています[9]。NECは、今後もブロックチェーンの動向を正確にとらえ、利活用する際の課題解決に取り組み、いち早く多くのユースケースにブロックチェーンを適用できるようにすることで、ビジネスの発展や豊かで明るい社会や未来を支える社会の実現に貢献していきます。

参考文献

1）情報処理学会誌2016年9月号　フィンテック特集 透明性と公平性を実現するブロックチェーン技術　佐古和恵（NEC セキュリティ研究所）
2）Ethereum Project
https://www.ethereum.org/
3）The Birth of Enterprise Ethereum in 2017
https://media.consensys.net/the-birth-of-enterprise-ethereum-in-2017-ebe7f7abed92
4）HYPERLEDGER FABRIC v1.0
http://hyperledger-fabric.readthedocs.io/en/latest/abstract_v1.html
5）The Hyperledger Project
https://www.hyperledger.org/
6）NEC プレスリリース：ブロックチェーン技術の活用に向けた研究会を発足
～事業コンソーシアム「Incubation & Innovation Initiative」と連携～
http://jpn.nec.com/press/201604/20160421_03.html
7）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」
http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html
8）NEC プレスリリース：NEC、三井住友信託銀行による信託業務へのブロックチェーン技術の活用に向けた実証実験を支援
http://jpn.nec.com/press/201610/20161025_02.html
9）Gartner®「先進テクノロジのハイプ・サイクル：2016年」
https://www.gartner.co.jp/press/html/pr20160825-01.html

執筆者プロフィール

鳥山 慎一
金融システム開発本部
マネージャー

宮岸 聖高
金融システム開発本部
主任

並木 悠太
クラウドプラットフォーム事業部
主任

小出 俊夫
セキュリティ研究所
主任研究員

関連URL

NEC 金融ソリューション：ソリューション・サービス
http://jpn.nec.com/financial/index.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.69 No.2　デジタルトランスフォーメーションを加速するFinTech特集

デジタルトランスフォーメーションを加速するFinTech特集によせて
NECが目指すFinTechの全体像

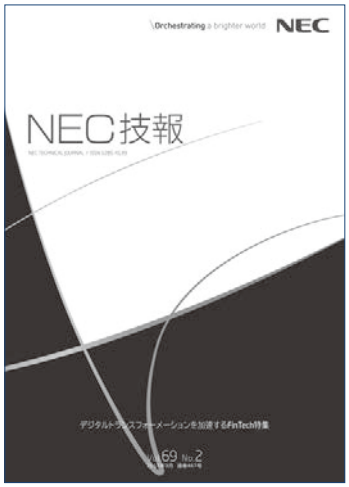
◇ 特集論文

FinTech時代の新しい金融と技術の関係
AIがもたらす金融サービスの変革
ブロックチェーンによる企業間連携の実用化に向けた取り組み
ロボットとAIの組み合わせによる顧客コミュニケーションの高度化
ウェアラブルデバイスを用いた安全・安心・便利な見守りサービス
生体認証によるモバイルサービスのセキュリティと利便性の両立
新たなサービスのスピーディな提供を可能にするモバイルアプリ高速開発
サイバーセキュリティ対策推進による金融サービスの安全性向上
FinTechのセキュリティ強化に貢献するマルチパーティ計算技術

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2016　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2016年度C&C賞表彰式開催



Vol.69 No.2
（2017年3月）

特集TOP