ブロックチェーン技術の可能性と課題への取り組み

山田 仁志夫 Yamada Nishio
佃 美和 Tsukuda Miwa
根本 潤 Nemoto Jun
長沼 健 Naganuma Ken
西島 直 Nishijima Nao
佐藤 竜也 Sato Tatsuya

互いに信頼のない不特定多数の利用者間での直接的な取引をセキュアに実現することにより，取引コストの削減をねらう革新技術として，ブロックチェーンが注目を浴びている。日立は，これまでミッションクリティカルシステムの構築で培ってきたセキュリティ技術や分散データ処理技術を活用し，ブロックチェーンの研究開発を推進している。本稿は，ブロックチェーンのユーザー企業とのディスカッションで特に注目が高かった課題を述べ，課題に対する日立の取り組みを概観する。Hyperledgerプロジェクトでのコミュニティ活動を通じて，ブロックチェーンの標準化基盤を開発するとともに，高信頼化機能を開発し，社会インフラに適用可能なブロックチェーンの実現をめざす。

1. はじめに

従来，金融機関や政府など信頼できる第三者機関を経由して実施されてきた取引を，利用者間（P2P：Peer to Peer）での直接的な取引に代替することで，コストの大幅な削減が期待できる革新技術として，ブロックチェーンが注目を浴びている。現状では，ハイプサイクルの黎（れい）明期を過ぎ，流行期のピークを過ぎた辺りに位置づいており，多くのベンダやユーザー企業は，個別に実証実験を行い，ブロックチェーンの課題を洗い出すとともに，実適用に向けて独自にブロックチェーン技術の強化を行っている。今後予想されるハイプサイクルの幻滅期を乗り越え，ブロックチェーンの適用範囲をさらに拡大させるためには，乱立するブロックチェーン技術の標準化を行い，金融と物流の連携や，IoT（Internet of Things）デバイスと連携した少額決済など，業種をまたがるユースケースを実現するための技術開発が必要である。また，金融や公共など，社会インフラを支えるシステムにブロックチェーンを適用するにあたっては，現状では課題が多いブロックチェーンの高信頼化が必須である。

本稿では，ブロックチェーンのユーザー企業である金融機関や関連省庁との議論を重ねてきた結果として，ブロックチェーンに対する課題を述べる。次に，課題に対する日立の取り組み方針を述べ，Linux FoundationのHyperledgerプロジェクトでのコミュニティ活動と，高信頼化機能開発の取り組み事例を紹介する。

2. ブロックチェーンの特徴と課題

2.1 ブロックチェーンの特徴

ブロックチェーンは，暗号通貨であるBITCOIN※）の実装技術として注目されている。現状では，BITCOINのブロックチェーンが持つ以下（1）～（3）の設計思想をベースに，さまざまな派生技術が提案され，進化を続けている。

（1）ブロックチェーンネットワーク上の利用者間（P2P）取引において第三者機関を介することなく，参加者が承認することによって取引を確定させる。

（2）複数の取引をブロックとしてまとめ，数珠つなぎに分散元帳に記録する。連続するブロックにハッシュ計算を施すことにより，改ざんを実質不可能にする。

（3）参加者全員が同一元帳データを共有することにより，参加者全員での取引の確認を可能とする。

2.2 ブロックチェーンの課題

日立は，これまでブロックチェーンの適用を検討している金融機関や省庁など50以上のユーザー企業と議論を重ねてきた。**表1**に議論となった上位5つの課題を示す。

ほぼすべてのユーザー企業との議論で，プライバシー保

※）BITCOINは，株式会社bitFlyerの登録商標である。

表1｜ブロックチェーンの課題

ユーザー企業との議論を通じて注目度が高かった課題の上位5つを示す。主に，プライベート領域での課題を示す。

No.	課題
1	利用者のプライバシー保護
2	処理速度，単位時間当たりの処理件数
3	処理の確定（ファイナリティ）
4	既存システムとの連携
5	ブロックチェーンの信頼性

護，処理速度，処理の確定の3点が議論となった。これらはセキュリティやシステム性能といった非機能面の課題である。ブロックチェーンのデータが全ネットワーク参加者で共有されるため，全データを分析すれば，例えば，支払元から支払先への送金金額を追跡できる可能性がある（同表No.1）。取引を承認し，元帳の一貫性を維持するための処理時間を要するため，単位時間当たりの処理件数が少なくなる（同表No.2）。また，取引の承認時にPoW（Proof of Work）と呼ぶ承認アルゴリズムを利用する場合は，時間の推移とともに取引確定の確率は高まる方式となり，厳密には取引が確定しない（同表No.3）。

また，ブロックチェーンの適用を小さく始め，段階的に拡大したいという意見が多く，ブロックチェーンどうしの連携や，ブロックチェーンと既存システムとの連携が課題である（同表No.4）。さらに，将来的にブロックチェーンが本格稼働した際のシステムの信頼性に関して同数の議論があった（同表No.5）。例えば，システムの連続稼働やデータベースの拡張可能性などである。

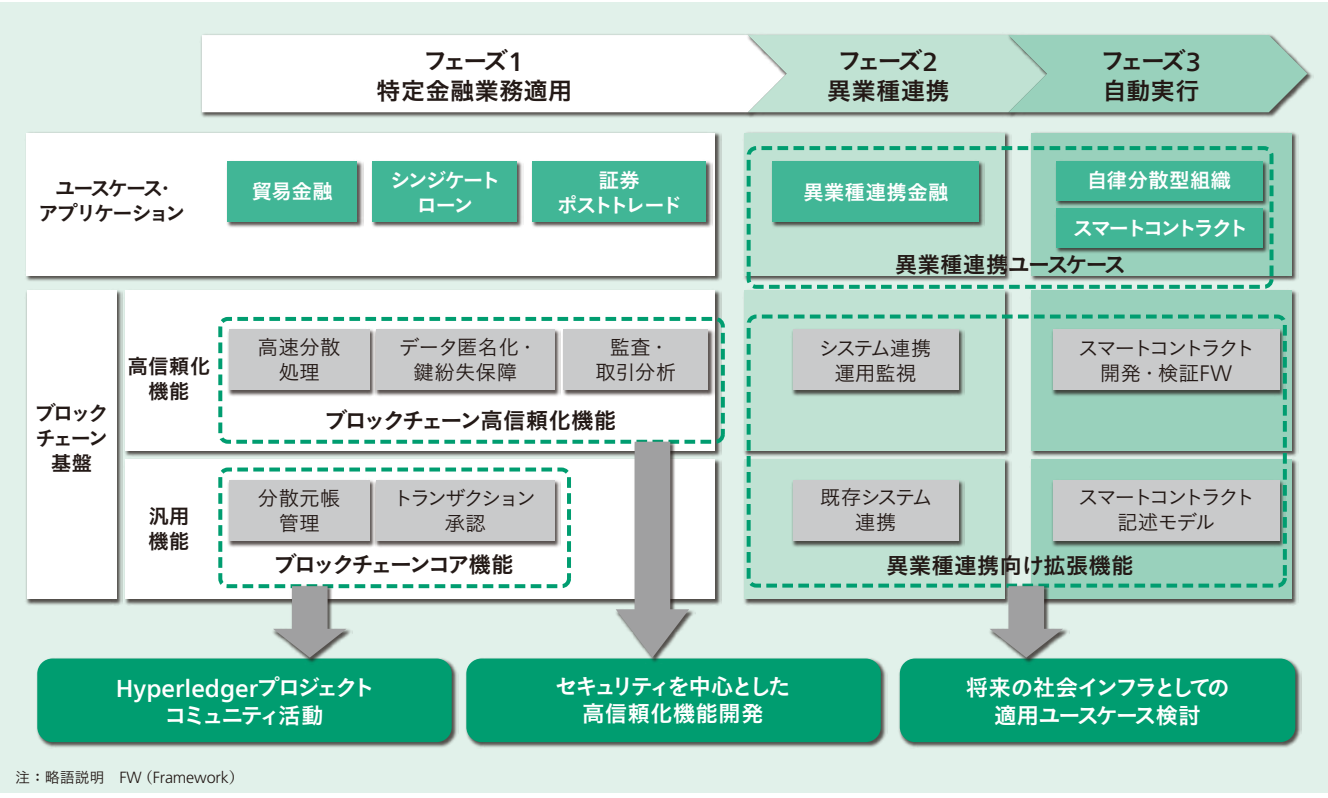
3. 日立の取り組み

3.1 取り組み方針

日立は，大きく3つのフェーズに分けてブロックチェーンの適用を拡張する方針である（**図1**参照）。

フェーズ1では，ブロックチェーンへの取り組みが活発化している金融分野を対象に，シンジケートローンや証券ポストトレードといった特定業務への適用を検討し，ブロックチェーン基盤が提供する機能の検証と強化を図る。具体的には，分散元帳管理やトランザクション承認といったブロックチェーン基盤が提供するコア機能は，Hyperledgerプロジェクトのコミュニティ活動を通じて，グローバル標準の機能開発を推進する。一方，金融インフラには高い信頼性が求められ，前章の課題でも述べたとおり，非機能面を中心に，ブロックチェーン基盤機能の強化が必須である。金融基幹系システムの構築ノウハウやセキュリティ，データ処理技術など研究成果を活用した実証実験を通じて，データ匿名化や監査機能など，金融インフラへの適用に向けた高信頼化機能を開発する。

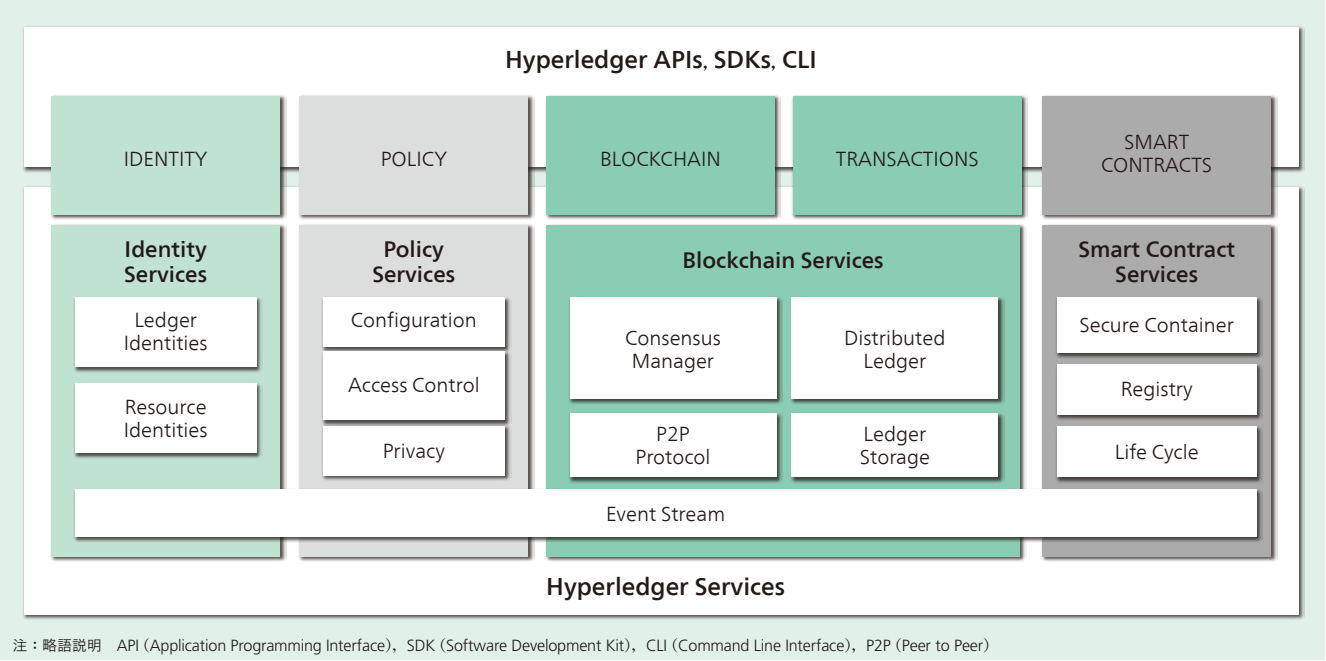
フェーズ2以降では，物流やヘルスケアといった異業種と金融の連携，また，自律分散型組織の実現に向けたIoTやAI（Artificial Intelligence：人工知能）を絡めたスマート



注：略語説明　FW（Framework）

図1｜日立の取り組み方針

特定の金融業務へのブロックチェーン適用から，異業種連携，スマートコントラクトを活用した自動実行へと拡大していく。



注：略語説明　API（Application Programming Interface），SDK（Software Development Kit），CLI（Command Line Interface），P2P（Peer to Peer）

図2｜Hyperledgerで開発する基盤のアーキテクチャ
大きく5つの構成要素から成る。

コントラクトなど，日立の幅広い事業ドメインの知識を活用しながら，将来の社会インフラを支える異業種連携ユースケースを模索する。ブロックチェーンと既存システムの連携機能や，スマートコントラクトが仕様どおりに正しく実装されていることを検証する機能など，本ユースケースを実現するための異業種連携向け拡張機能を開発し，ブロックチェーン基盤のさらなる高信頼化を実現する。

3.2　Hyperledgerコミュニティ活動

(1) コミュニティ活動概要

Linux Foundationは，2016年2月にオープンソースソフトウェアのブロックチェーン基盤の開発を目的としたHyperledgerプロジェクトを設立した。日立は，同プロジェクト設立時からプレミアメンバーとして参画し，DTCCやJPMorgan Chase & Co.といった参加企業と協働で，ユースケースの検討やブロックチェーンの基盤開発といったコミュニティ活動を推進している。具体的には，米国サンタクララに設立した金融イノベーションラボに在籍する研究者が，国内の開発者と連携しながら，技術検討を行うテクニカルステアリングコミッティに参加し，ブロックチェーン標準化基盤の開発に貢献している。

(2) アーキテクチャ

ブロックチェーンを適用するユースケースに応じて，求められる基盤の要件が異なるため，Hyperledgerプロジェクトは，基盤機能を極力モジュール化する方針で開発を進めている。ユースケースの要件に応じて，必要なモジュールを切り替えることで，開発のスピードが向上し，コストを低減させることが可能となる。

Hyperledgerで開発するブロックチェーン基盤のアーキテクチャは大きく5つの構成要素から成る（図2参照）。主

表2｜アーキテクチャ構成要素の概要
図2の構成要素の概要を示す。

構成要素名	説明
Identity Services	ブロックチェーンネットワークへの参加者，スマートコントラクト，コンセンサスを実施する検証ノードなど，ネットワーク上のすべてのオブジェクトのIDを管理する。
Policy Services	各種ポリシーを管理する。アクセス制御や権限管理に加え，参加者のプライバシー，コンセンサスのルールなどを管理する。
Blockchain Services	P2Pプロトコル，分散台帳，コンセンサスマネージャといった要素によって構成される。 ・P2Pプロトコル: P2Pでの双方向ストリーミング，フロー制御，リクエストの多重化といった機能を提供する。既存ネットワークと連携して動作する。 ・分散台帳: ブロックチェーンと，状態を管理する。 ・コンセンサスマネージャ: プラグイン可能なコンセンサスアルゴリズム用のインタフェースを提供する。例えば，PBFTのインタフェースを提供する。
Smart Contract Services	検証ノード上でスマートコントラクトを実行する手段を提供する。セキュアな実行環境とスマートコントラクトのライフサイクル（配備～更新～停止）管理機能を含む。
Event Stream	Pub/Sub型のイベント管理機能を提供する。例えば，外部システムが分散台帳上のイベントを検知することなどを可能にする。
API	上記の各構成要素に対するAPIを提供する。また，外部公開用APIも整備する。

注：略語説明　PBFT（Practical Byzantine Fault Tolerance），Pub/Sub（Publish/Subscribe）

要構成要素およびその他の概要を**表2**に示す。取引の承認に関しては，PBFT（Practical Byzantine Fault Tolerance）と呼ぶ合意形成アルゴリズム，あるいはPBFTを拡張したアルゴリズムを採用している。これらは，前章で述べた課題のうち，取引の確定[3]を解決するものである。

(3) 今後の方針

Hyperledgerでは，以下 (a)，(b) などの機能拡張を予定している。(a) は，前章で述べた課題のうち，ブロックチェーンの信頼性を，(b) は，既存システムとの連携の解決をねらった取り組みの一つである。

(a) PBFTは，取引の承認をつかさどる検証ノードの数を固定する必要があり，システムの連続稼働に対する要望を満たせないことが課題であった。Hyperledgerでは，検証ノード数を動的に変更可能なPBFTアルゴリズムを開発する。

(b) ユーザー企業がこれまで開発してきた既存システムを，ブロックチェーンでそのまま置き換えることはコストやスケジュール面で難しく，既存システムとブロックチェーンを連携させる機能が必須となる。ブロックチェーンどうしの連携機能に加え，既存システムとブロックチェーンとを連携させる機能を開発する。

3.3 高信頼化機能の開発

Hyperledgerプロジェクトでのコミュニティ活動と並行して，ブロックチェーンの金融インフラ適用に向け，日立の強みであるセキュリティ技術や分散処理技術を活用した高信頼化機能を開発している。

セキュリティ技術を活用した高信頼化機能としては，ユーザー企業の注目度が高い利用者のプライバシー保護の課題解決に向け，データ匿名化機能を開発している。これは，ゼロ知識証明と呼ぶ暗号方式を利用し，ブロックチェーンのデータを匿名化するものであるが，ブロックチェーン上のすべてのデータを分析したとしても，第三者による送信者と受信者の対応づけを不可能にするとともに，特定の監査者にのみ，送信者と受信者の対応づけを可能とする特徴を持つ。

また，ブロックチェーンでは，鍵を紛失すると，ブロックチェーン上で取引ができなくなる。仮想通貨の例では，通貨の所有者は取引が行えず，通貨が失われてしまうことを意味する。本課題に対して，生体認証を利用した鍵紛失保障機能を開発している。秘密鍵を紛失した際も，生体認証を用いて秘密鍵と公開鍵証明書を再発行することで，継続的な取引を実現する。

その他，動的にノード追加が可能なPBFTアルゴリズムの開発に加え，システム連続稼働を支援するためのシステムモニタリング機能や，ブロックチェーンデータの容量拡張性を確保するためのスケーラブルデータストアの開発を進め，システムのさらなる高信頼化をめざす。

4. おわりに

本稿では，ユーザー企業との議論で明確化したブロックチェーンの課題を述べ，課題に対する日立の取り組みを述べた。今後，金融インフラへのブロックチェーン適用に向けて，Hyperledgerプロジェクトでの標準化基盤の開発を着実に推進するとともに，さらなる高信頼化に向けて機能拡張を推進し，将来の社会インフラを形作る異業種連携ユースケースを支えるブロックチェーン基盤の開発をめざす。

参考文献など

1) S.Nakamoto : Bitcoin: A Peer-to-Peer Electronic Cash System (2009.11)
2) Hyperledger Projectホームページ, https://www.hyperledger.org/
3) Fabric Wiki, https://github.com/hyperledger/fabric/wiki

執筆者紹介

山田 仁志夫
日立製作所 研究開発グループ システムイノベーションセンタ
システム生産性研究部 所属
現在，ブロックチェーン基盤およびアプリケーション開発の生産性向上の研究に従事
経営情報学会会員，情報処理学会会員

佃 美和
日立製作所 金融ビジネスユニット 金融システム営業統括本部
事業企画部 金融イノベーション推進センタ 所属
現在，ブロックチェーン・人工知能（EMIEW3＋リモートブレイン）の企画・立案に従事

根本 潤
日立製作所 研究開発グループ 情報通信イノベーションセンタ
ストレージ研究部 所属
現在，ストレージシステムやブロックチェーンの研究開発に従事
情報処理学会会員

長沼 健
日立製作所 研究開発グループ システムイノベーションセンタ
セキュリティ研究部 所属
現在，情報システムのセキュリティ技術開発に従事
日本医療情報学会会員

西島 直
日立製作所 研究開発グループ 北米社会イノベーション協創センタ 所属
現在，ブロックチェーン基盤およびクラウドサービスの研究開発に従事

佐藤 竜也
日立製作所 研究開発グループ 情報通信イノベーションセンタ
クラウド研究部 所属
現在，ブロックチェーン基盤およびクラウドサービスの研究開発に従事
情報処理学会会員，IEEE会員