

---

# ブロックチェーン技術の活用可能性と課題 に関する検討会報告書

－ ブロックチェーン技術が銀行業務に変革をもたらす可能性を見据えて －

---

2017年3月16日

ブロックチェーン技術の活用可能性と課題に関する検討会

（事務局：一般社団法人 全国銀行協会）

## 序文

近年、金融とテクノロジーの融合（FinTech）の動きが進展するなか、今後の銀行業務・システムに変革をもたらし得る有力なテクノロジーの一つとして、「ブロックチェーン技術」に対する注目が高まっている。

ブロックチェーン技術は、一般に、「取引履歴を暗号技術によって過去から1本の鎖のようにつなげ、ある取引について改竄を行うためには、それより新しい取引について全て改竄していく必要がある仕組みとすることで、正確な取引履歴を維持しようとする技術<sup>1</sup>とされる。同技術を活用したシステムは、データの破壊・改竄が極めて困難であること、実質的なゼロ・ダウンタイム・システムが実現できる可能性があること等の特長があることから、今後、金融分野に限らず、様々な業務やシステムへの応用が期待されている<sup>2</sup>。

こうした中、ITの進展を金融分野に取り込むこと等により、金融サービスの高度化を図り、利用者利便の向上やわが国経済の成長力強化につなげていく観点から、「金融審議会決済業務等の高度化に関するワーキング・グループ報告～決済高度化に向けた戦略的取組み～」(2015年12月22日公表)や政府「日本再興戦略2016-第4次産業革命に向けて-」(2016年6月2日閣議決定)等において、ブロックチェーン技術の活用可能性と課題について、銀行界と金融行政当局等が連携して検討していく方針が打ち出されている。

一般社団法人全国銀行協会では、これを受け、銀行界、IT事業者、FinTech企業、ブロックチェーン業界団体、金融インフラ運営機関、弁護士、学識経験者、関係当局等をメンバーとする「ブロックチェーン技術の活用可能性と課題に関する検討会」を設置し、同検討会において、銀行分野におけるブロックチェーン技術の活用可能性と課題について検討を行った。

本報告書は、同検討会の成果として、銀行業務におけるブロックチェーン技術の活用可能性と課題を考察するとともに、同技術が銀行業務に変革をもたらす可能性を見据え、実用化に向けて官民連携して必要となる取組みを提言するものである。

<sup>1</sup> 金融審議会決済業務等の高度化に関するワーキング・グループ報告(2015年12月22日)5頁。

<sup>2</sup> World Economic Forumのサーベイによれば、2027年までに世界のGDPの約10%がブロックチェーン技術上で記録されるとの見方もある(World Economic Forum “Deep Shift: Technology Tipping Points and Societal Impact”, 2015.9)。

## 目次

1. はじめに .....	8
1.1 本報告書の目的 .....	8
1.2 本報告書の前提とするブロックチェーン技術／分散型台帳技術（DLT） ...	8
2. ブロックチェーン技術／DLTの基本的な仕組み .....	10
2.1 基本的な仕組み .....	10
2.2 要素技術 .....	11
2.3 形態分類 .....	13
3. ブロックチェーン技術／DLTの活用可能性を巡る国内外の検討状況 .....	15
3.1 全体像 .....	15
3.2 個別の取組概要 .....	16
3.2.1 R3 .....	16
3.2.2 Hyperledger Project .....	17
3.2.3 Ripple .....	17
3.2.4 その他 .....	17
4. 銀行分野におけるブロックチェーン技術／DLTの活用可能性と課題 .....	19
4.1 活用上の論点 .....	19
4.1.1 機能に関する論点 .....	19
4.1.2 システムの安定性・セキュリティに関する論点 .....	21
4.1.3 データの秘匿性確保に関する論点 .....	22
4.1.4 実装上の論点 .....	24
4.1.5 費用対効果に関する論点 .....	25
4.2 銀行分野における活用に向けた着眼点 .....	26
4.2.1 為替取引 .....	27
4.2.2 KYC .....	28
4.2.3 勘定系システム .....	28
4.2.4 金融インフラ .....	29
4.2.5 その他 .....	32
5. ブロックチェーン技術／DLTが銀行業務に変革をもたらす可能性を見据えて .....	33
5.1 官民挙げた取組みの必要性 .....	33
5.2 検討会提言（「ブロックチェーン官民連携イニシアティブ」） .....	33
5.2.1 銀行界における「ブロックチェーン連携プラットフォーム」（仮称）の整備 .....	33
5.2.2 国際的な標準規格への対応戦略 .....	34
5.2.3 金融インフラにおける活用可能性の検討 .....	35
5.2.4 ブロックチェーン技術／DLTの活用に向けた関係当局との連携 .....	36
5.2.5 ブロックチェーン技術／DLTの活用に向けた中央銀行との連携 .....	36
5.2.6 安全対策基準の適用関係に関する整理 .....	36
5.2.7 ブロックチェーン・コミュニティの形成 .....	37

## ブロックチェーン技術の活用可能性と課題に関する検討会名簿

メンバー	中山 知章	(株) 三井住友銀行 IT イノベーション推進部長
	柏木 英一	(株) 三菱東京UFJ銀行デジタルイノベーション推進部長
	阿部 展久	(株) みずほフィナンシャルグループインキュベーションPT長
	梅原 弘充	(株) 静岡銀行理事経営企画部長
	佐々木 勉	(株) 北洋銀行チャネル開発部フィンテック推進室長
	吉本 憲文	住信SBIネット銀行(株) FinTech 事業企画部長
	増田 豊	全国銀行資金決済ネットワーク(全銀ネット) 事務局長
	内田 浩示	(株) 全銀電子債権ネットワーク(でんさいネット) 代表執行役社長
	赤羽 喜治	(株) NTTデータ金融事業推進部技術戦略推進部システム企画担当部長
	貝塚 元彦	日本アイ・ピー・エム(株) インダストリー・ソリューションズ ブロックチェーン部長
	加納 裕三	日本ブロックチェーン協会代表理事 / (株) bitFlyer 代表取締役
	杉井 靖典	ブロックチェーン推進協会副代表理事 / カレンシーポート(株) 代表取締役 CEO
	沖田 貴史	FinTech 協会 / SBI Ripple Asia(株) 代表取締役
	荻生 泰之	デロイトトーマツコンサルティング合同会社執行役員
	松浦 幹太	東京大学生産技術研究所教授
	岡田 仁志	国立情報学研究所准教授
	片岡 義広	片岡総合法律事務所 所長弁護士
	木下 信行	アフラックシニアアドバイザー
	井上 俊剛	金融庁総務企画局信用制度参事官
	小林 寿太郎	金融情報システムセンター企画部長
	永沢 裕美子	Foster Forum 良質な金融商品を育てる会事務局長
オブザーバー	岩下 直行	日本銀行決済機構局審議役 FinTech センター長
	山藤 敦史	(株) 日本取引所グループ総合企画部フィンテック・ラボ課長
事務局	一般社団法人全国銀行協会	

(敬称略)

## 開催概要

報告書の取りまとめに当たっては、以下の会議体を設置して討議を行った<sup>3</sup>。

### ブロックチェーン技術の活用可能性と課題に関する検討会

- ・ 検討の方向性や検討会傘下に設置した研究会から提出された報告書案について、ハイレベルで討議を行うための会議体。

### ブロックチェーン技術の活用可能性と課題に関する研究会

- ・ 報告書案について実務的、専門的な討議を行うための会議体。

上記検討会および研究会の主な開催概要は以下のとおりである。

#### 2016年8月4日 第1回研究会

- ・ 事務局説明「本研究会で取組むテーマに関する問題提起」
- ・ 事務局説明「全銀協アンケート調査の結果について」

#### 2016年12月20日 第1回検討会

- ・ 事務局説明「ブロックチェーン検討会報告書の方向性について（案）」
- ・ 事務局説明「諸外国におけるブロックチェーン技術の活用可能性に係る検討状況」
- ・ 事務局説明「全銀協アンケート調査の結果について」
- ・ NTT データ「ブロックチェーン技術の特長と課題」
- ・ 日本 IBM「決済でのブロックチェーン活用と留意点」
- ・ デロイトトーマツコンサルティング「ブロックチェーン研究会<sup>4</sup>における取組」

#### 2017年1月25日 第2回研究会

- ・ 事務局説明「ブロックチェーン技術の活用可能性と課題①」
- ・ 全銀ネット「全銀システムのご紹介とブロックチェーン技術活用の課題」
- ・ でんさいネット「でんさいネットの概要とブロックチェーンの応用にあたっての課題」
- ・ SBI Ripple Asia「Ripple Solution 概要及び内外為替一元化コンソーシアムに関して」
- ・ 住信 SBI ネット銀行「ブロックチェーン実証実験概要」

<sup>3</sup> いずれも事務局は一般社団法人全国銀行協会。

<sup>4</sup> 株式会社みずほフィナンシャルグループ、株式会社三井住友銀行、株式会社三菱 UFJ フィナンシャル・グループ、デロイトトーマツグループで構成される研究会。なお、一般社団法人全国銀行協会を事務局とする「ブロックチェーン技術の活用可能性と課題に関する研究会」とは別の私的研究会。

2017年2月3日 第3回研究会

- ・ 事務局説明「ブロックチェーン技術の活用可能性と課題②」
- ・ 片岡弁護士「ブロックチェーン技術と金融機関関連の法制度的論点について」<sup>5</sup>

2017年2月20日 第4回研究会

- ・ 事務局説明「ブロックチェーン検討会報告書（案）について」
- ・ デロイトトーマツコンサルティング「ブロックチェーン技術の活用による金融業界への影響」

2017年3月8日 第2回検討会

- ・ 事務局説明「ブロックチェーン検討会報告書（案）について」
- ・ 日本銀行「BIS 決済・市場インフラ委員会による報告書『支払・清算・決済における分散型台帳技術—分析的枠組み—』について」<sup>6</sup>

各検討会／研究会において、有益な示唆の提供やプレゼンテーションにご協力いただいた関係者の皆様には、この場を借りて、深く感謝申しあげる。

---

<sup>5</sup> 配付資料は、片岡総合法律事務所ウェブサイト  
([http://www.klo.gr.jp/lawyers/dat/yk170316\\_paper.pdf](http://www.klo.gr.jp/lawyers/dat/yk170316_paper.pdf)) をご参照。

<sup>6</sup> 配付資料は、日本銀行ウェブサイト  
([http://www.boj.or.jp/announcements/release\\_2017/rel170228b.htm/](http://www.boj.or.jp/announcements/release_2017/rel170228b.htm/)) に同一資料を掲載。

## 要 旨

- ・ ブロックチェーン技術／分散型台帳技術（Distributed Ledger Technology。以下、DLT）は、今後の銀行業務・システムに大きな変革をもたらす可能性を秘めており、現在、国内外の様々な金融機関等において実用化に向けた検討が進められている。わが国銀行界でも、現在、多くの銀行において、実証実験をはじめとする様々な活用可能性の検証・検討が行われているところである。
- ・ 他方、銀行のシステムでは、高い安定性、信頼性、正確性が求められ、同技術の実用化には、現状、技術面のほか、運用面、セキュリティ面や法制度面等、様々な点についてさらなる検討が必要とされる。
- ・ ブロックチェーン技術／DLT の「分散型台帳」という特性や、銀行業務には銀行間ネットワークを前提とする取引、業務が多いこと、共通化することでコスト削減が可能な業務が存在すること等を踏まえれば、これらの課題の解決に向けては、個別行ベースの競争的な取組みに加え、官民の関係者による連携した取組みも同時に進めていくことが重要である。
- ・ こうした観点から、当検討会は、官民の関係者に対し以下の取組みを提言する。

### 「ブロックチェーン官民連携イニシアティブ」

#### ① 銀行界における「ブロックチェーン連携プラットフォーム」（仮称）の整備

ブロックチェーン技術／DLT の活用可能性の検討が、個別行単独の検討から銀行間で連携・協働したコンソーシアム型の検討フェーズに移りつつあることを踏まえれば、銀行界を中心に、連携・協働型の実証実験環境として「ブロックチェーン連携プラットフォーム」（仮称）の来年度中を目途とした整備に向けた検討を進めることが期待される。こうした環境整備を行うことにより、例えば、新たな決済・送金サービスやKYC、金融インフラ（全銀システム、でんさいネットシステム等）等、ブロックチェーン技術／DLT の活用が期待される分野について、実用化に向けた積極的な検討が進められることが期待される。

#### ② 国際的な標準規格への対応戦略

将来的に海外金融機関との連携・協働も視野に入れた新たなサービスや仕組み等を検討するに当たっては、国際的な普及可能性等も考慮したブロックチェーン技術／DLT 基盤の選択が重要となる。銀行界における「ブロックチェーン連携プラットフォーム」（仮称）の整備に向けては、国際的な標準規格を巡る動向や各基盤の特徴にも留意しつつ、相応しいブロックチェーン技術／DLT 基盤を検討・選定のうえ、取組みを先進的に進めていくことが期待される。

#### ③ 金融インフラにおける活用可能性の検討

金融インフラ（でんさいネットシステムや全銀システム等）については、将来的なインフラの改善やコスト低減等の可能性を見据え、先取的に活用可能性の検討をスケジュール感をもって進めていくことが重要である。将来的な金融インフラとしての役割・立ち位置等も見据えつつ、各金融インフラ運営機関においては、これらの取組みを遅滞なく果敢に進めていくことが期待される。でんさいネットシステムにおいては、「ブロックチェーン連携プラットフォーム」（仮称）における実証実験も視野に、システムの抜本的な効率化を目指した取組みを進めていくこと、また、全銀システムにおいても、ブロックチェーン技術／DLT の活用について継続的に検討を行っていくことが期待される。

#### ④ ブロックチェーン技術／DLT の活用に向けた関係当局との連携

実用化を目指した実証実験を行う場合、開発するプログラムや仕組み、ビジネスルール等は、最終的な法制度への準拠も視野に検討を進めていく必要がある。関係当局においては、個々の実証実験や実用化に向けた検討における法制度面の論点整理について積極的に支援すること等を通じて、ブロックチェーン技術／DLT の実用化に向けた民間の取組みを後押ししていくことが期待される。

#### ⑤ ブロックチェーン技術／DLT の活用に向けた中央銀行との連携

中央銀行においては、決済の安全性確保や効率性向上等の視点を踏まえ、金融インフラ等へのブロックチェーン技術／DLT の活用の取組みについて、銀行界等と対話していくことが期待される。また、そうした取組みを国際的な決済を巡る議論との整合性を確保しつつ進めていく観点から、ブロックチェーンを巡る国際的な議論の動向等を銀行界等に随時還元していくことが期待される。

#### ⑥ 安全対策基準の適用関係に関する整理

情報セキュリティ関連機関においては、安全対策上の責任面および技術面から、実証実験の動向やユースケースの出現状況等を睨みながら、ブロックチェーン技術／DLT に係る調査・研究を進めるとともに、改訂が予定されている新たな安全対策基準を前提に、その適用関係（解釈・運用等）を整理することが期待される。

#### ⑦ ブロックチェーン・コミュニティの形成

IT 事業者、ブロックチェーン関係団体／事業者、学者・研究者、関係当局等の幅広い関係者に、銀行分野における活用上の課題について理解を促し、課題解決や実用化に向けた更なる研究、技術開発等を促していく必要がある。こうした観点から、銀行界においては、銀行間の連携・協働した実証実験を後押ししていくとともに、実証実験を通じて得られた研究成果の概略や技術動向等について業界全体でシェアする枠組み等の整備等を通じて、コミュニティ形成を促していく取組みが期待される。また、学術研究の分野においても、更なる研究の推進と研究成果の共有、本分野の研究者の育成等が積極的に進められることが期待される。

# 1. はじめに

## 1.1 本報告書の目的

本報告書は以下を目的とする。

- ・ 現在、個別行レベルで把握されている活用上の課題や有識者の知見等を集約し、検討会として、銀行分野におけるブロックチェーン技術の活用可能性と課題について整理すること。
- ・ これらを対外公表することによって、IT 事業者、ブロックチェーン関係団体／事業者、学者・研究者、関係当局等の幅広い関係者に、銀行分野における活用上の課題について理解を促し、課題解決や実用化に向けたさらなる調査・研究、技術開発等を促していくこと。
- ・ ブロックチェーン技術が銀行業務・システムに変革をもたらす可能性を見据えつつ、実用化に向けて官民連携して必要となる取組みを提言すること。

なお、ブロックチェーン技術は、今後、銀行分野に限らず、例えば、証券取引や不動産登記等の様々な業務やシステムへの応用が期待されているが、本報告書では特に銀行分野に焦点をあてて検討を行う。

## 1.2 本報告書の前提とするブロックチェーン技術／DLT

ブロックチェーン技術とは、一般に、「取引履歴を暗号技術によって過去から1本の鎖のようにつなげ、ある取引について改竄を行うためには、それより新しい取引について全て改竄していく必要がある仕組みとすることで、正確な取引履歴を維持しようとする技術」<sup>7</sup>とされる。

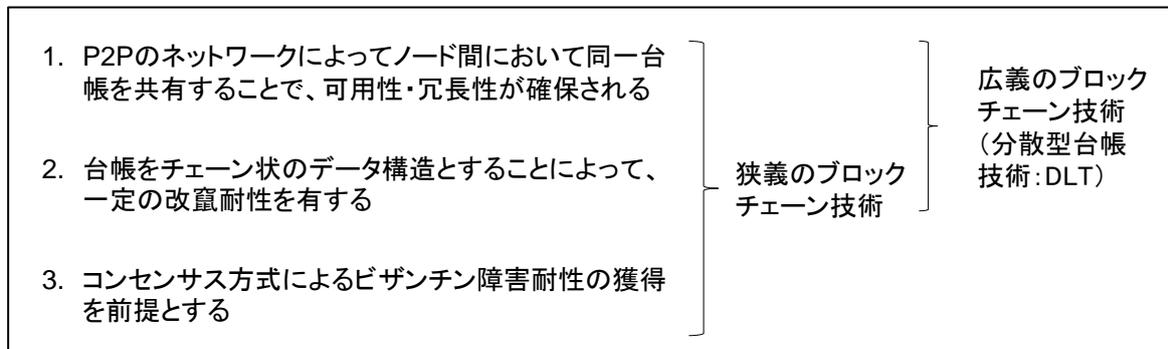
ブロックチェーン技術には、目的に応じて様々な形態が存在し、銀行分野における同技術の活用可能性の検討においては、ビットコインをはじめとする仮想通貨の技術基盤である狭義のブロックチェーン技術のみならず、目的に応じて、同技術の有益な技術的特徴を部分的に取り出した広義のブロックチェーン技術（いわゆる分散型台帳技術：Distributed Ledger Technology：以下、DLT）についても、活用可能性の検討が行われている。

---

<sup>7</sup> 金融審議会決済業務等の高度化に関するワーキング・グループ報告（2015年12月22日）5頁、脚注7。なお、国際的に広く合意された定義は存在しない。

これらを踏まえ、本報告書では以下のブロックチェーン技術／DLT の活用可能性と課題について検討を行う。

**【図表 1】本報告書が対象とするブロックチェーン技術／DLT の基本的な範囲**

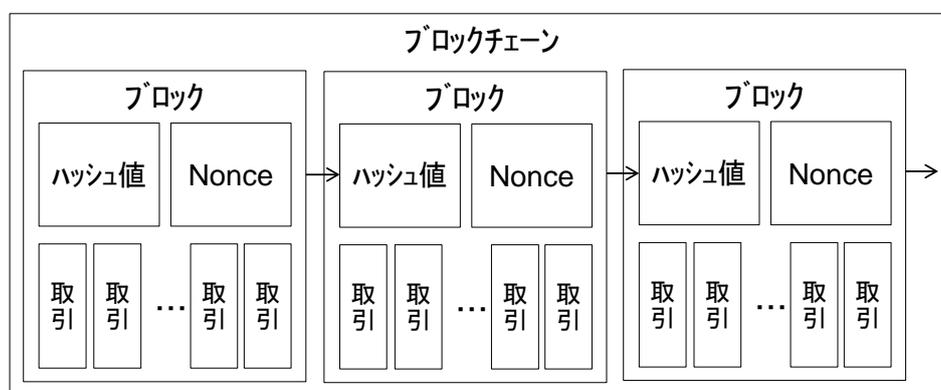


## 2. ブロックチェーン技術／DLTの基本的な仕組み

### 2.1 基本的な仕組み

ブロックチェーンでは、取引履歴（ブロック）が暗号技術によって過去から1本の鎖のようにつなげるかたちで記録される。一つのブロックは、合意された取引記録の集合体と、各ブロックを接続させるための情報（「ハッシュ値」や「Nonce」等）で構成される。ブロックチェーンとは、このブロックが複数連結されたものを指す。

【図表2】ブロックチェーンの基本的な仕組み



ハッシュ値とは、ハッシュ関数<sup>8</sup>を用いた計算によって前のブロックが持つ情報から生成された値である。仮に、新しいブロックに前のブロックそのものを包含するとブロックの連結が起こる度にファイルサイズが増大するが、ハッシュ値を用いることでファイルサイズの増大を抑制することができる。このハッシュ値により、ブロックの順序性を維持することが可能となっている<sup>9</sup>。

Nonceとは、新しいブロックを作成する際にハッシュ計算に与えられるパラメータである。PoW（Proof of Work、詳細は12頁参照）においては、新たなブロックの生成に、計算負荷の大きい、予め定められた条件を満たすNonceの発見作業（マイニング）を課すことで、ブロックの改竄を困難としている。

ある参加者が何らかの取引を行った場合、当該取引内容は、P2Pネットワークの分散環境上の全参加ノードに通知される（ブロードキャスト）。当該取引内容が、

<sup>8</sup> 与えられた原文から固定長の疑似乱数を生成する演算手法をいう。

<sup>9</sup> ただし、ハッシュ値から前のブロックが持つ情報を生成することはできない。

予め取り決められた方法（コンセンサスアルゴリズム<sup>10</sup>）によって承認されると新たなブロックが生成される。

ブロックチェーン技術を支える分散型台帳の仕組みでは、参加者である複数システムがそれぞれ台帳データを保有し、常に同期が取られる。仮に複数のユーザーが同時に同じデータに対して書込要求をした場合、一般的なデータベースは一方の要求を抑止して他方の要求を処理する（排他制御）が、分散型台帳では、コンセンサスアルゴリズムによって、どの要求を優先的に反映させるかが決定される。

## 2.2 要素技術

ブロックチェーン技術／DLTは、複数の要素技術を組み合わせた技術であり、主には、①分散型台帳、②スマートコントラクト、③偽造防止・暗号化技術、④コンセンサスアルゴリズム、⑤P2Pネットワーク等によって構成される。

### ① 分散型台帳

ブロックチェーン化された取引記録は、通常の集中管理型システムと異なり、P2Pネットワークの参加者によってそれぞれ保持される（分散型台帳）。従来の技術では複数参加者で同一の情報を保持することに制約があったが、ブロックチェーン技術／DLTでは、改竄できない状態で同一の情報を共有することが可能となる。

### ② スマートコントラクト

スマートコントラクトとは、広義にはプログラム化され自動的に実行可能とされた契約であり、狭義にはブロックチェーン／分散型台帳上で動作するエージェントプログラムを指す。ブロックチェーン／分散型台帳を個々の業務領域に対応させるうえでは、スマートコントラクトを業務要件にあわせて記述する。

### ③ 偽造防止・暗号化技術

偽造防止、暗号化技術は、取引情報をネットワーク上に流す際に、自らの取引であることを証明するために公開鍵暗号方式を用いて電子署名し、ハッシュ関数で計算するといったかたちで利用される。

### ④ コンセンサスアルゴリズム

コンセンサスアルゴリズムは、分散環境上の複数のノードによって単一の結果に

---

<sup>10</sup> 共有するデータの正当性を保証し、一意に特定する仕組みであり、様々な種類がある（詳細は次頁を参照）。

ついて合意形成する際に生じる問題を解決するために利用される。コンセンサスアルゴリズムには様々なものが存在し（詳細は【BOX1】を参照）、ブロックチェーン／分散型台帳の活用目的、業務要件に応じて適切なものを選択する。

## ⑤ P2P ネットワーク

ブロックチェーン／分散型台帳は、特定の管理主体が存在するクライアント＝サーバ型ではなく、特定のサーバやクライアントを持たずに、各参加ノードが対等に直接通信する P2P ネットワーク上で維持される。

### 【BOX1】 主なコンセンサスアルゴリズムとその特徴

#### Proof of Work (PoW)

多大な計算量が必要な問題を最初に解いた者がブロックを作成できる仕組み。大量の参加ノードにも対応できる特徴がある。同時に複数のブロックが作成された場合、参加ノード内の多数派が認めたブロックを正とすることで分散環境特有の問題を回避している。ただし、P2P ネットワーク上での情報共有においては参加ノード間でタイムラグが生じることから、ファイナリティを完全には確定できない<sup>11</sup>。例えば、今まで正としていたブロックとは別のブロックが多数派に認められた場合は、当該ブロックを無効とし、別のブロックに切り替えなければならない（チェーンに分岐が生じ得る）。また、承認まである程度の時間がかかるため、リアルタイム性にも欠ける。

#### Proof of Stake (PoS)

「大量の資産を所有する参加者は、その価値を守るために、システムの信頼性を損なうことはしない」という推定概念にもとづき、資産量をより多く所有する承認者が優先的にブロックを作成できる特徴を持つ。これによって、ハッシュ計算の負荷が下がり、PoW と比較してリソース消費が小さくなるというメリットがある。ファイナリティが確定できない（チェーンに分岐が生じ得る）点やリアルタイム性に欠ける等の課題は PoW と基本的に同一である。

#### Proof of Importance (Pol)

仮想通貨 NEM (New Economy Movement) に採用されているコンセンサスアルゴリズム。ネットワークに対するユーザーの「重要度」によってブロックが生成される。重要度は、アカウント内の残高と過去の取引数にもとづき決定される。悪意ある行為を予防するため、残高や取引数の計算方法についてルールが設けられており、高額な残高を持っているだけでは重要

<sup>11</sup> ビットコインでは PoW が用いられており、新たなブロックを一つ作るために 10 分を要する設計とされている。ファイナリティの判定は、ある取引がブロックチェーンに記載されてから、さらに 6 ブロック生成されることで、慣例的に確定したと取り扱われる。

度が上がらない仕組みとなっており、PoS に比べより複雑な優先順位決定が行われる。ファイナリティの確保に関しては、PoW、PoS と同一の課題がある（チェーンが分岐し得る）。ただし、重要度に従ってブロックの生成が行われるため、PoW と比較して性能（処理速度等）は比較的確保しやすくなる。

### Practical Byzantine Fault Tolerance(PBFT)

ネットワーク上の参加者の 1 人がプライマリ（リーダー）となり、自らを含む全参加者に要求を送り、その要求に対する結果を集計して多数を占めている値を採用することでブロックを確定させる方式のアルゴリズム。ブロックの確定に必要なノード数は予め定められており、不正なノード数を  $f$  とすると全体のノード数は  $3f+1$  必要となる。参加者の増加に伴い合意形成に要するメッセージ量が指数関数的に増えるとともに、合意形成の時間も長期化するため、通常は上限を必要とする（一般的には 10~20 の参加者が適当とされる）。合意を得てからブロックを生成するため、チェーンの分岐が生じず、PoW や PoS の弱点である分岐後のファイナリティ判定の不確実性を解消することが可能。Hyperledger Fabric や Eris 等のコンソーシアム型を想定したブロックチェーン基盤において採用されている。

## 2.3 形態分類

ブロックチェーン／分散型台帳は、参加者の公開範囲・制限内容によって、①パブリック型、②コンソーシアム型、③プライベート型の 3 つの形態に分類される。これらは、ユースケースに応じて適切な形態が選択され、また、公開範囲に制限を加えることによって、より金融機関のユースケースに適したコンセンサスアルゴリズムの採用が可能となる。

### ① パブリック型

誰でも参加可能なオープンなブロックチェーン／分散型台帳。悪意のある者が参加するリスクを排除できないため、一般に、悪意のある者が改竄等を行うインセンティブを削ぐコンセンサスアルゴリズムの採用を必要とする。ブロックチェーンの活用事例の中でもよく知られるビットコインは、パブリック型の一例である。

### ② コンソーシアム型

一定の条件を満たす者のみが参加資格を有する形態のブロックチェーン／分散型台帳。参加者を信頼できる者に限定することで、悪意のある者が参加するリスクを低減し、よりユースケースに適した（例えば、処理速度の速い、ファイナリティが確保できる）コンセンサスアルゴリズムの採用が可能となる。一般に、エンタープライズ領域における活用に適する。

### ③ プライベート型

単一組織内（社内システム等）で運営する形態のブロックチェーン／分散型台帳。社外の者との間で情報共有を行わないため、情報の秘匿性の確保が可能となる。主には集中管理型システムの代替として利用が検討される。

【図表3】ブロックチェーン／分散型台帳の形態分類

	パブリック型	コンソーシアム型	プライベート型
管理主体	管理者が存在せず	複数組織	単一組織
参加	自由	許可制	
コンセンサス アルゴリズム	PoW 等、悪意のある参加者を前提とする方式	PBFT 等の分散コンセンサス形成アルゴリズム (悪意のある参加者を前提としないコンセンサスアルゴリズムの採用が可能)	
ファイナリティ	チェーンが分岐し、ファイナリティが不確定となる (確率的となる)	PBFT 等のコンセンサスアルゴリズムを採用することで、ファイナリティを確保することが可能	

### 3. ブロックチェーン技術／DLT の活用可能性を巡る国内外の検討状況

#### 3.1 全体像

ブロックチェーン技術／DLT は、今後の銀行業務・システムに大きな変革をもたらす可能性を秘めており、現在、国内外の様々な金融機関等において実用化に向けた検討が進められている<sup>12</sup>。

こうした検討は、2016年頃まで、実証実験等を通じた技術的な検証やプロトタイプを試作といった取組みが中心となっていたが、2017年に入り、実用化に向けた検討フェーズに入ったプロジェクトも見られ始めている。IBM社が行った調査<sup>13</sup>によれば、世界主要金融機関200行のうち、14%が2018年までにブロックチェーン技術／DLTを実用化、70%が2020年までに実用化を見込んでいる。

【図表 4-1】 主なブロックチェーン技術／DLT の活用検討分野

分類	主要な取組の傾向	実証実験例	実用化例	
金融サービス	通貨	仮想通貨発行に留まらず、決済を円滑化する中央銀行向け通貨や、企業独自の通貨やポイントの発行が加速	【仮想通貨】 UBS、Deutsche、 BNY Mellon、 Santander	【仮想通貨】 ビットコイン
	送金・決済	決済時間の短縮が求められ即時性が必ずしも求められない「国際送金」への取組が世界中で特に活発	【国内送金】 SMBC、みずほ、 MUFG	【国際送金】 Santander (Ripple)
	融資	契約条項の履歴管理や、一連の取引記録の管理として期待される、「貿易金融」や「シンジケートローン」の分野での取組が中心	【シンジケート ローン】 みずほ	【貿易金融】 KBC Bank (ベルギー)
	金融商品取引	速度を求められない未公開株取引、債券取引の実現や、業務効率化が期待されるポストトレード等の取組が中心	【ポストトレード】 BoA、Citi、 JPMorgan、 Credit Suisse	【未公開株取引】 Nasdaq
金融情報管理	個人情報管理、企業情報管理、KYC等、金融機関が持つ情報を統合したインフラの新規構築、既存更改	【企業情報管理】 Kompany.com	【KYC】 ConsenSys	

(資料) 第4回研究会デロイトトーマツコンサルティングプレゼンテーション資料

<sup>12</sup> 邦銀においても、一般社団法人全国銀行協会が2016年6～7月に実施した会員へのアンケート調査によれば、回答銀行99行中66行(約67%)の銀行が、調査・研究活動も含めて何らかの検討を行っている」と回答している。

<sup>13</sup> IBM Institute for Business Value “Leading the pack in blockchain banking”(2017)。

【図表 4-2】各国金融機関の主なブロックチェーン技術／DLT の活用検討状況

		送金・決済	貿易金融	債券等取引	ローン取引	デリバティブ取引	行内インフラ等	コンプライアンス	その他
地域	北米	Citigroup JPMorgan Chase Wells Fargo ANZ, SWIFT VISA	Bank of America 欧米15 金融機関	BNP Paribas	JPMorgan Chase Digital Asset Holdings		BNY Mellon State Street		BNY Mellon (BK coin) Goldman Sachs (SETLcoin, etc)
	欧州	CIBC RBC Barclays Santander Intesa Sanpalo	Bank of America, HSBC Barclays	CIBC Scotiabank State Street HSBC ING SocGen UBS UniCredit	US Bank Wells Fargo State Street Scotiabank BBVA RBS SocGen等	DTCC Bank of America Citigroup JPMorgan Credit Suisse Barclays	Citigroup HSBC Credit Suisse 等 ABN Amro BNP Paribas	US Bank Northern Trust CIBC ING BBVA Nordia SocGen UBS等	CME Group LSE SocGen UBS等 (証券決済) BNP Paribas (ホストレード)
	日本 アジア	MUFG みずほ SMBC SMBC, MUFG みずほ, テロ付 りそな等 47行 ふくおかFG	Standard Chartered DBS 静岡 オリックス SMBC	MUFG	みずほ SMBC		住信SBI	楽天証券 ソラミツ	みずほ (クロスボーダー証券 決済) MUFG (電子契約書)

各金融機関が単独で取組んでいる事例 (IT企業等との連携を含む)  
 コンソーシアム等複数金融機関が連携して取組んでいる事例

(資料) 各種報道・プレスリリースにもとづき作成

## 3.2 個別の取組概要

### 3.2.1 R3

R3 は、米・金融ベンチャーの R3CEV 社が中心となって、新技術を活用した金融業向けインフラの構築や法規制への対応等の研究を目的に 2015 年 9 月に設立されたコンソーシアムである。2016 年 12 月現在、同コンソーシアムには、Barclays、BBVA、J.P. Morgan、UBS、Bank of America、Deutsche Bank、HSBC、三菱 UFJ フィナンシャル・グループ、みずほフィナンシャルグループ、三井住友銀行、野村證券等の 70 社以上が参画している<sup>14</sup>。

これまでに発表された主な活動には、「Ethereum」プラットフォームを用いた DLT の可能性の検証や、「Chain」、「IBM 社の基盤」、「Intel 社の基盤」、「Ethereum」、「Eris」の 5 つの異なるプラットフォームを用いた債権（コマーシャルペーパー）の発行・二次市場における取引・償還等に関する実証実験、共有型 KYC<sup>15</sup> サービスの実証実験等がある。ただし、現時点においては、いずれのケースも本番環境での稼働には到達していない。

R3 コンソーシアム主導で金融業界向けの分散型台帳基盤「Corda」が開発され、2016 年 11 月にオープンソース化された。

<sup>14</sup> <http://www.r3cev.com/press/2016/12/14/credicorp-joins-r3-distributed-ledger-consortium>

<sup>15</sup> Know Your Customer、顧客管理の意。

### 3.2.2 Hyperledger Project

Hyperledger Project は、ブロックチェーン技術／DLT の推進を目的として、2016年2月に創設されたコンソーシアムである。Linux Foundation が中心となり、日本を含む世界の30以上のIT企業や金融機関等が協力して研究、開発を推進している。

R3では金融業に特化した活動を行っているのに対し、Hyperledger Projectでは、製造業や保険、不動産契約、IoT、ライセンス管理、エネルギー取引等、様々な業界の要件に対応することを目的とする。

Hyperledger Project で開発された基盤を活用した取組みとしては、UBS を中心とする貿易金融領域における実証実験、日本取引所グループによる証券分野に関する実証実験<sup>16</sup>がある。また、みずほフィナンシャルグループが、2016年6月にHyperledger Fabric を用いて、決済業務の領域における仮想通貨等の検証作業を行うと発表している<sup>17</sup>。

### 3.2.3 Ripple

Ripple は、2012年に米サンフランシスコで設立されたフィンテックベンチャー。ブロックチェーンに代表される分散技術等を活用し、安全性が高く、低コストの、小口・高頻度の国際決済にも耐え得る新たな決済インフラの構築を目指している。

グローバル銀行の上位50行のうち15行が、Rippleの構築した国際決済ネットワークに参加、もしくは参加を表明しており、グローバルベースで90以上の銀行が、実証実験(PoC)を完了している。また、Rippleが発行する仮想通貨XRPは、銀行間決済におけるブリッジカレンシーとして活用する方法も可能であり、R3においても12行が参加し、XRPの活用に関する実証実験を完了している。

わが国においても、Rippleを基盤技術として採用する「内外為替一元化コンソーシアム」が、2016年10月に設立されており、2017年3月現在、47の金融機関が参加している。

### 3.2.4 その他

このほか、現時点で各金融機関または複数金融機関の連携によって行われている主なブロックチェーン技術／DLTの活用可能性の検討状況は、次頁のとおり。

---

<sup>16</sup> [http://www.jpix.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX\\_working\\_paper\\_No15.pdf](http://www.jpix.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf)

<sup>17</sup> [https://www.mizuho-fg.co.jp/release/20160622release\\_jp.html](https://www.mizuho-fg.co.jp/release/20160622release_jp.html)

【図表5】わが国金融機関の主な活用可能性に関する検討状況

発表日	実施行（参加行）	概要
2015年12月	住信 SBI ネット銀行	ブロックチェーン技術を活用した将来の基幹・業務システム構築を目的とした実証実験を開始
2016年2月	みずほ フィナンシャルグループ	国内企業4社との協働によるサプライチェーン業務を対象とした実証実験を開始
2016年2月	みずほ フィナンシャルグループ	海外ITサービスプロバイダーとの協働による、国境を越えた複数国間の文書情報共有ならびに独自通貨の実証実験を開始（※2017年2月に完了）
2016年3月	みずほ銀行	富士通と国境を越えた証券取引の決済プロセス効率化に向けた実証実験を実施
2016年3月	ふくおか フィナンシャルグループ	ポイント交換や各種決済サービス等の新たな金融サービスへの適用可能性に向けた検証を開始
2016年6月	みずほ フィナンシャルグループ	決済業務におけるブロックチェーンの適用可能性および仮想通貨の実現性についての評価等を開始
2016年7月	みずほ フィナンシャルグループ	R3 コンソーシアムにおける協働プロジェクトとしてブロックチェーンを活用した国際送金の実証実験を開始
2016年7月	静岡銀行 オリックス銀行	貿易金融をテーマとしたブロックチェーン適用に関する実証実験を完了
2016年8月	三菱東京 UFJ 銀行	シンガポールにおいて、小切手の電子化を対象としたブロックチェーン技術活用の実証実験を開始
2016年11月	みずほフィナンシャルグループ、三菱UFJフィナンシャルグループ、三井住友銀行（ブロックチェーン研究会）	国内の銀行間振込業務におけるブロックチェーン技術の実証実験を実施
2016年11月	山陰合同銀行	ブロックチェーンを活用した電子マネーの実証実験を開始
2017年1月	岩手銀行	ブロックチェーン技術を活用したサービスの実証実験を開始
2017年2月	三井住友銀行	貿易分野におけるブロックチェーン技術の適用可能性に関する実証実験開始

（資料）各銀行プレスリリースにもとづき作成

（注）銀行界における全ての取組みを網羅したものではなく、報道等があったものでも、プレスリリース等で正式な発表が確認できないものは除外している。

## 4. 銀行分野におけるブロックチェーン技術／DLTの活用可能性と課題

### 4.1 活用上の論点

既存または新たに開始する業務・取引について、集中管理システムとブロックチェーン技術／DLTのいずれが適するかは、業務・取引ごとの性質や特性等によって区々であるが、銀行分野においてブロックチェーン技術／DLTを活用するに当たっては、同技術の性質に起因する以下が論点となる<sup>18</sup>。

【図表6】ブロックチェーン技術／DLTの活用上の論点

分類	論点
① 機能	✓ 性能要件・データ同期 ✓ ファイナリティ
② システムの安定性・セキュリティ	✓ ゼロ・ダウンタイム（可用性・冗長性） ✓ 改竄耐性・不可逆性、トレーサビリティ
③ データの秘匿性確保	✓ 取引記録の共有および管理 ✓ 暗号化・権限管理
④ 実装時	✓ 運用・ガバナンス ✓ リソース・容量
⑤ 費用対効果	

現在、銀行業務・取引は、集中型のシステム・データベース（集中管理システム）によって管理されることが一般的であり、ある業務・取引に関してブロックチェーン技術／DLTの活用可能性を検討するに当たっては、こうした論点について、集中管理システムと比較したブロックチェーン技術／DLTの優位性について検証していくことになる<sup>19</sup>。

#### 4.1.1 機能に関する論点

##### 4.1.1.1 性能要件・データ同期

- ・ コンセンサスアルゴリズムおよびその処理速度は、処理性能を決める主要因となることが多い。遅すぎると性能要件を満たさず、速すぎると同期・承認等の

<sup>18</sup> 法制度面の課題については、末尾【参考資料2】をご参照。

<sup>19</sup> なお、本節は、ブロックチェーン技術／DLTの一般的な特性として記載している。日進月歩で技術革新が進む本領域において解決が試みられている課題もあることから、個別の製品においては当てはまらない場合があることに留意されたい。また、各論点は相互に関係する場合があり、必ずしも独立した論点とは限らない。ある論点の課題を解消するための対策が、他の論点に影響を与える場合がある。

処理にシステムや通信の負荷が大きくなるため、業務や取引に応じて両者のバランスを考慮したコンセンサスアルゴリズムやシステムの設計が必要となる。

- チェーンの分岐が発生しないコンセンサスアルゴリズム（PBFT等。以下同じ）では、ブロックチェーン／分散型台帳参加者の実行結果を集計するよう設計されるため、処理の遅い参加者が存在する場合や参加者数が多い場合、全体として合意形成に時間がかかり、想定する業務や取引の実運用に必要な処理速度が確保できない場合がある。チェーンの分岐が発生し得るコンセンサスアルゴリズム（PoW、PoS、PoI等。以下同じ）を採用する場合、ブロックチェーン／分散型台帳参加者が多いほど、同期のタイムラグによって分岐が増加し、一時点における参加者間におけるデータ不整合が多発する可能性が高くなる。
- コンピュータ性能の向上に伴って処理性能を改善していくためには、単位時間あたりに共有するデータ量を増やしていく等のプログラムの機能拡張が必要となるが、特にパブリック型ブロックチェーンでは、参加者の過半数以上の合意を必要とするため、仕様変更が難しく、コンピュータ性能の向上等の技術進歩が処理性能の改善に必ずしも結びつかなくなる可能性がある。
- 一般に、処理性能は、セキュリティや可用性とトレードオフの関係にある。例えば、パブリック型ブロックチェーンでは、参加者の増加は可用性の向上を意味するが、システム設計を工夫しなければ処理性能が低下する可能性がある。

#### 4.1.1.2 ファイナリティ

- ファイナリティ（決済完了性）とは、一般に、「決済が無条件かつ取消不能となり、最終的に完了した状態」を指す<sup>20</sup>。チェーンの分岐が発生し得るタイプのコンセンサスアルゴリズムは、多数のノードの参加にも対応しやすいという特徴を有するが、半面、その仕組み上、取引内容が覆る可能性を完全にゼロにできない（ファイナリティが確保できない）<sup>21</sup>。そのため、決済機能を提供する金融サービス等にブロックチェーン技術／DLTを活用するうえでは、取引の安全性や安定性の観点から、ファイナリティとの関係が重要な論点となる。
- この問題に関しては、現状の現預金取引の考え方を踏まえ、以下のような点について整理しておく必要がある。

<sup>20</sup> ただし、①当事者間完了性、②対第三者完了性、③資金決済完了性、④支払指図の撤回不可能性等、多義的に用いられることも多い。詳細については、嶋拓哉「資金決済におけるファイナリティ概念について」（<http://www.fsa.go.jp/frtc/nenpou/2006a/11.pdf>）を参照。

<sup>21</sup> 例えば、ビットコインでは、ある取引について、ブロックに記録されてから、さらに6ブロック生成されると確定したものとみなしている（6ブロック未満でも確定とみなす事業者もある）に過ぎず、一定の確率で取引が覆る可能性が残される。

- 取引完了とみなす時点
  - 取引内容が覆った場合の対処方法
  - 取引の実施時刻の確定方法
  - ある参加者により取引が受け付けられたものの、障害等により記録がなされなかった場合の対処方法や回復方法
- ・ チェーンの分岐が発生しないコンセンサスアルゴリズムでは取引内容が覆る可能性はないが、障害等により一部のノードで情報が遅延した場合等には、台帳の内容に齟齬が生じる場合がある。その時点で台帳の情報を読み出した場合、ノード間でのデータの一貫性が担保されない可能性がある。
  - ・ システム設計により、取引がブロックに記録されるまでに意図せず長時間を要する場合や取引の受付順とブロックに記録される順に齟齬が起こる可能性があり、サービスが確実に実行されるか否かの予見可能性が低くなる場合がある<sup>22</sup>。

#### 4.1.2 システムの安定性・セキュリティに関する論点

##### 4.1.2.1 ゼロ・ダウンタイム（可用性・冗長性）

- ・ ブロックチェーン技術／DLT では、複数の参加者（ノード）それぞれにおいて同一の情報（台帳）が共有されるため、一部の参加者の台帳が停止・故障しても<sup>23</sup>、システム全体の運行・稼働に与える影響を抑制することができる。このため、ブロックチェーン技術／DLT では、一般に、可用性、冗長性の高い（実質的なゼロ・ダウンタイム）システムの実現が比較的容易とされる<sup>24</sup>。
- ・ ブロックチェーン／分散型台帳自体が無停止であっても、周辺システムやサービスに停止時間があれば、可用性は制限される。また、参加者が減少した場合、冗長性、可用性は維持されても、改竄耐性に影響が生じる。
- ・ 高い冗長性、可用性確保と引き換えに、分散型システムでは、参加者がクライアントの役割もサーバの役割も果たさなければならず、加えて障害発生時には自律的に役割を変更し、多数での意思決定処理を行わなければならない。そのため、集中管理システムと比べ、一般にその動作は複雑となる。

##### 4.1.2.2 改竄耐性・不可逆性、トレーサビリティ

<sup>22</sup> 例えば、ビットコインでは、手数料が高い取引が優先的に承認され、低い取引が承認されない（72 時間経過した場合は記録が消滅）等の事象が存在する。

<sup>23</sup> ただし、ブロックチェーン／分散型台帳は多数決により信頼性を担保しているため、データの信頼性確保に必要な人数を下回った場合等の対処については運用方法を考える必要がある。

<sup>24</sup> なお、可用性の確保に必要な条件（稼働台数等）は、コンセンサスアルゴリズムや参加形態（プライベート型、パブリック型、コンソーシアム型）等によって様々である。

- ・ ブロックチェーン／分散型台帳は、改竄耐性・不可逆性が確保しやすいデータ構造を持つ。このため、集中管理システムと同水準の改竄耐性・不可逆性を、より単純な構成、低コストで実現できる可能性がある。ただし、改竄耐性の水準は、コンセンサスアルゴリズムによる影響を受け、業務要件に応じた方式の採用が必要となる。
- ・ ブロックチェーン技術／DLT を用いることで、取引のトレーサビリティと透明性が向上し、監査証跡として利用できる可能性がある。
- ・ 高い不可逆性によって事後修正が難しくなるため、技術面・運用面から、誤った情報が書き込まれた場合の修正・取消方法や台帳に記録する情報の信憑性を担保する方法についても別途検討が必要となる。
- ・ コンセンサスアルゴリズムによっては、ブロックチェーン／分散型台帳を構成するコンピュータ資源（CPU 等）のうち、一定割合以上を占める参加者（群）が存在する場合、その参加者（群）が事実上のブロックチェーン／分散型台帳の管理運営者となり、意図的に台帳を改竄するリスクがある<sup>25</sup>。

#### 4.1.3 データの秘匿性確保に関する論点

##### 4.1.3.1 取引記録の共有および管理

- ・ ブロックチェーン技術／DLT の、複数の参加者それぞれにおいて同一の情報（台帳）を共有する特性は、参加者間での情報共有を前提とする（あるいはそれによって何らかの付加価値が生まれる）業務や取引等においては利点となる。
- ・ 一方、参加者間での情報共有を前提としない業務・取引では、以下が論点となり得る。
  - 取引当事者でない参加者が台帳記録を保持することに関する法的整理
  - ブロックチェーン／分散型台帳参加時における情報共有要領
  - ブロックチェーン／分散型台帳脱退時における情報の確実な削除方法
- ・ ブロックチェーン／分散型台帳では、取引受付とその記録時刻が乖離し得るほか、一般的に分散システムでは参加者間で完全には時刻が一致しない。そのため、時刻の記録方法や各状態における時刻の解釈について予め参加者間の合意と法的整理を必要とする。
- ・ 全参加者での同一情報の保持を確認するためには、全参加者からの確認応答が

<sup>25</sup> このため、ブロックチェーン参加者の特性を継続的に把握する必要性とその方法や、ブロックチェーン参加者の極端な増減を回避する方法について、別途検討が必要となる。

必要であり、集中管理システムと比較して一般に即時性に制約がある。参加者間の不整合を認める方法もあるが、チェーンが分岐する等の別の課題が生じる。

#### 4.1.3.2 暗号化・権限管理

- ・ ブロックチェーン／分散型台帳は、複数の参加者でそれぞれが同じ情報(台帳)を共有する方式であるため、台帳に記録された情報は、原則、参加者全員に開示される。権限管理と暗号化によって取引の一部や全部を秘匿することも可能であるが、情報の閲覧が可能な参加者を取引当事者に限定したい場合の情報秘匿化技術は、現状開発途上にある。また、暗号化技術の実装は、処理性能とのトレードオフとなるため、処理性能に与える影響についても考慮が必要となる。
- ・ これらの各種セキュリティ要件について、例えば以下の技術を組み合わせた実現方法が提案されている。

【図表7】セキュリティに関する技術動向

セキュリティ要件	実現方法
ユーザー認証	ユーザーIDとログインによりユーザーを認証。
トランザクション認証	電子証明書の仕組みにより、それぞれのトランザクションをどのユーザーが実行したかを認証。
プライバシー保護	匿名証明書により、トランザクション実行者を匿名化。
データの秘匿化	トランザクションの内容を暗号化。
アクセス制御	ユーザーごとに、実行可能なトランザクションや、データへのアクセス権限(Read/Write)を制限。

- ・ 暗号化によって取引当事者以外に秘匿しても、参加者全員で暗号化された情報自体は共有されるため、法的論点の整理が必要となる。また、集中管理システムと比べて、より多くの関係者がブロックチェーン台帳／分散型台帳を保持することから、暗号解読試行者の手に渡る機会が従来よりも増え、暗号解読のリスクが高まってしまう<sup>26</sup>。
- ・ 権限を集中管理するために集中管理システムを利用する場合、記録台帳自体に可用性・冗長性が確保されていても、当該集中管理システムが単一障害点となる可能性がある。
- ・ 現在の最新技術によって暗号化しても、将来的なコンピュータ性能向上や暗号

<sup>26</sup> ただし、R3コンソーシアム主導で開発された分散型台帳基盤“Corda”では、データを当事者以外に保有させない等の対策が図られている。もっとも、この場合、秘匿性の面で安心感が高まるが、可用性の面では課題が生じる。

解読技術の進歩により、現在の暗号技術ではセキュリティが不足（危殆化）する事態も想定され、長期間運用が前提となるシステムでは対策が必要となる。

#### 4.1.4 実装上の論点

##### 4.1.4.1 運用・ガバナンス

- ・ ブロックチェーン／分散型台帳は、複数の参加者でそれぞれが同じ情報（台帳）を共有する方式であるため、集中管理システムと比べて、全体で見れば運用・管理の当事者が増加し、運用・ガバナンスが複雑となる。
- ・ ブロックチェーンのもつ不可逆性に起因して、一度ブロックチェーン上に配置したプログラムは変更できない。どのように変更、修正に対応するか、対策を講じる必要がある。
- ・ 関係者において、例えば、以下の事項について予め合意が必要となる。
  - プログラムの仕様決定方法や更改方法
  - ブロックチェーン／分散型台帳の参加者が増減する場合の手続、処理内容
  - インセンティブの運用プロセス（特に PoW の場合）
  - 障害発生時や脅威顕在時の運用方法（復旧や原因究明）
  - システム運用費の分担方法
  - コンソーシアム型の場合、参加者の選定基準や KYC の方法
  - 情報の確定時期等についての取扱い
  - ブロックチェーン／分散型台帳の記録に沿った取引が実行されなかった場合の対応や法的措置
  - 実システム運用開始後の保守のための実環境を模した試験環境の要否、仕様
- ・ ブロックチェーン／分散型台帳の運用状況（参加者、台帳の同期状況、コンセンサスの速度、等）を常時監視する方法についても検討が必要となる。

##### 4.1.4.2 リソース・容量

- ・ ブロックチェーン／分散型台帳は、自身の関係しない取引を記録する必要があることから、台帳の保持に必要な情報容量が参加者の増加に比例して増加するため、情報容量について、集中管理システムと比べて、大容量の見積りが必要となる<sup>27</sup>。
- ・ 情報容量に係るリソース制約を緩和するためには小容量化技術のさらなる開発

---

<sup>27</sup> ただし、R3 コンソーシアム主導で開発された分散型台帳基盤“Corda”ではこの点について解決が図られている。

が必要となる。

- ・ コンセンサスアルゴリズムによっては、合意形成に多くのコンピュータ資源や電力を必要とするものがあり、合意形成に必要な資源は、台帳運営コストとして、ブロックチェーン／分散型台帳の参加者が負担することになる。特にコンソーシアム型の場合、不公平感のないリソース分担について検討が必要となる。
- ・ 集中管理システムに比べ、システム増強による処理高速化が難しい傾向にある。特にパブリック型は、コンセンサスアルゴリズムによっては、参加者数に応じて処理性能やファイナリティに影響を与える<sup>28</sup>。

#### 4.1.5 費用対効果に関する論点

- ・ 銀行業務で利用されるシステムでは、冗長性や可用性の確保、改竄対策、トレーサビリティの確保等が重要な考慮事項となることが多い。これらの要件を満たすため、従来の集中管理型システムでは、システムの多重化等の対応を行っているが、ブロックチェーン技術／DLTでは、同要件を比較的 low コストで満たすことができる可能性があると言われている。そのため、同技術の活用によって、銀行システムの抜本的な効率化が可能になることが期待されている。
- ・ ただし、コスト比較に当たっては以下の点についても留意が必要となる。
  - 集中管理システムにおいても、ホストコンピュータのオープン系コンピュータへの移行、クラウド化といったコスト低減策が存在するため、他のコスト低減策との比較検討が必要となる。
  - コスト比較においては、合意形成に要するコストおよび台帳を最新状態に保つための通信コストの考慮が必要となる。
  - ブロックチェーン／分散型台帳を用いて新規システムを構築する場合、様々な要素を勘案し、システム・事務の運用面を含めた、TCO（総所有コスト）をもとにした検討が必要となる。
  - IT インフラだけでなく、インフラのあり方や業務プロセスの改革によるコスト削減効果についても検討が必要となる。
- ・ 集中管理システムをブロックチェーン技術／DLT を用いたシステムに移行する場合は、コストとの関係において、以下も論点となり得る。

---

<sup>28</sup> 例えば PoW では、参加者数が増えた場合、最初に条件に適する Nonce を発見する採掘者が早く現れるようになり、処理性能が向上する一方、通信負荷が増す（ただし、ビットコインでは、ブロック生成間隔が平均 10 分となるように、2 週間ごとに Nonce の条件が調整される）。PBFT では、必要数の承認が得られるまで待つため、必要数が増えれば処理性能は低下し、参加者数の増加に対して必要数を増やさない場合は、ビザンチン障害に対応しない。

- 移行範囲
- 社内外の周辺システムとの連携インタフェースや機能配置
- 既存の業務フローとの整合性
- 情報の保存形式の整合性<sup>29</sup>

## 4.2 銀行分野における活用に向けた着眼点

集中管理システムと比較したブロックチェーン技術／DLTの優位性は、ユースケースごとに異なるが、一般に、ブロックチェーン技術／DLTが適する業務・取引は以下とされる。

**【図表 8】 ブロックチェーン技術／DLT が適する業務・取引**

<p><b>〈適する業務・取引〉</b></p> <ul style="list-style-type: none"> <li>✓ 台帳を共有することにより何らかの価値が見出せる業務・取引 (分散型の情報連携、ビジネスプロセスの効率化、トレーサビリティの確保等)</li> <li>✓ リアルタイム性を求められない業務・取引</li> </ul> <p><b>〈不向きな業務・取引<sup>30</sup>〉</b></p> <ul style="list-style-type: none"> <li>✓ ミリ秒単位での高い処理速度が求められる取引</li> <li>✓ 一組織だけで構成される業務・取引 (通常システムで対応可能)</li> <li>✓ 単純なデータベース、ミドルウェア、トランザクション処理システムの代替</li> </ul>
--

銀行分野におけるブロックチェーン技術／DLTの活用にあたっては、これら特長と課題を踏まえつつ、ユースケースごとに最適な形態（パブリック型、コンソーシウム型、プライベート型）とコンセンサスアルゴリズムを選択することになる。

銀行分野の業務・取引に利用されているシステムは数多く存在するが、本節では、ブロックチェーン技術／DLTの活用可能性に関する実証実験や実用化に向けた検討が行われている、①為替取引、②KYC、③勘定系システム、④金融インフラの四つについて採り上げる。これらユースケースごとの主な活用可能性と留意点は、以下のとおりである。

なお、ブロックチェーン技術／DLTは現在、日進月歩で技術革新が進んでおり、

<sup>29</sup> ブロックチェーン／分散型台帳上に記録可能な情報の形式と、従来技術で保存していた情報の形式は、必ずしも同一にできない可能性がある。

<sup>30</sup> 不向きな業務・取引であっても、仕組み上の工夫等によって解決できる場合もあるため、必ずしも適用不可とは限らない。

現時点での技術水準にもとづくこと、これらは一般的な観点から考察したものであり、全ての活用可能性と留意点を網羅したものではないことに留意されたい。

#### 4.2.1 為替取引

##### ① 活用可能性に関する考察

内国為替取引に関しては、わが国では銀行間のリアルタイム送金の実現しているため、性能要件は基本的にはブロックチェーン技術／DLTの優位性とならない<sup>31</sup>。一方、ブロックチェーン技術／DLTでは、決済システムとして不可欠な高改竄耐性、高可用なシステムを低コストで実現できる可能性があるため、例えば一定の性能要件の低下を許容した安価な送金サービス（ロー・バリュー送金）の実現手段として活用できる可能性がある。また、付加機能のある送金サービスの提供を検討する場合は、既存システムの仕様の影響を受けず、かつ、参加者のイニシャル投資を比較的抑えやすい点で、ブロックチェーン技術／DLTの活用のメリットがあると期待される。

外国為替取引では、現在の性能要求水準を考慮すると、ブロックチェーン技術／DLTの処理性能でも同等以上の性能水準を達成できる可能性が高い。複数の仲介金融機関が介在し、情報（商流、金流）の中継を行っていることから、ブロックチェーン技術／DLTの「記録情報の共有および管理」という特色を活かし、オペレーションコストや手数料等の低減が期待される。また、ブロックチェーン／分散型台帳を銀行以外の事業者（サプライチェーン等）との間でも共有する仕組みとし、取引情報と決済を連動させることによって、トレードファイナンス等の分野で付加価値の高いサービスを開発・提供すること等も考えられる。従来はハードルの高かった国内外送金サービスの一体提供も展望できよう。

##### ② 留意点・課題

実用化に向けては、①技術的に実現可能な性能水準・機能と、②実装やデータの秘匿性確保に係るコストを含めたトータルの費用対効果の検証がポイントとなる。これらは、最終的に顧客が負担する送金コストに反映され、どのような送金サービスをどの程度の価格で実現できるかに影響することになる。

外国為替取引においてブロックチェーン／分散型台帳による仕組みの導入に際し、商習慣や法制度が異なる他国の事業者と連携する場合には、業務やシステムを含む様々な角度からの検証と合意が必要とされる。また、コンソーシアム型のブロ

---

<sup>31</sup> 他方、リアルタイム送金を実現できていない国では、性能水準次第で、ブロックチェーン技術／DLTが課題解決手段となり得る。

ックチェーン／分散型台帳ではネットワーク速度の影響が強く働くため、特に外国為替取引では、システムの慎重な動作検証を要する。

## 4.2.2 KYC

### ① 活用可能性に関する考察

現在、KYC<sup>32</sup>は、各銀行がそれぞれ行っており、銀行ごとに手続きが異なるケースもあることから顧客に手続負担が生じている。ブロックチェーン／分散型台帳の「情報の共有」、「高改竄耐性」という特長を活かすことで、銀行の壁を越えたタイムリーかつ正確な情報共有や、顧客手続負担の軽減等が実現できる可能性がある。情報のバックアップの面からも、ブロックチェーン／分散型台帳により分散管理が実現されれば、ハードウェア設備のコスト低減につながる可能性がある。

技術的な観点からみても、KYC情報は暗号化が必須とされるが、送金取引等と比較して高い処理性能が求められていないことから、通常発生するセキュリティと処理性能のトレードオフ関係の問題は発生しづらいと考えられる。

### ② 留意点・課題

KYC情報は、他のユースケースと比しても一般に高い情報の秘匿性確保が要求され、セキュリティ対策を含めこれに応える技術の開発が必要となる。顧客同意を前提として複数銀行間での情報共有を行う場合<sup>33</sup>、サービスの特性上、顧客の同意が得られるかが論点となる。

プライベート型、コンソーシアム型のいずれにおいても、法的論点の整理が必要となる。例えば、個人情報取り扱いにおける責任所在の明確化、参加者間の責任分界、問題解決方法のルール化等が考えられるが、それぞれ関連法令にもとづき検討する必要がある。

## 4.2.3 勘定系システム

### ① 活用可能性に関する考察

銀行の中核業務を処理する勘定系システムには、高い信頼性と安定性が求められるため、ブロックチェーン／分散型台帳の特長である高可用性を活かし、ゼロ・ダウンタイムが実現できれば、例えば、バックアップ装置等の削減等のコストメリットが生じる可能性がある。プライベート型を採用した場合、「運用・ガバナンス」

<sup>32</sup> 口座開設時の顧客情報および住所・氏名変更手続き時の更新情報、犯罪収益移転防止法上の取引時確認、外為法上の制裁対象者リスト等の管理等。

<sup>33</sup> 他方、KYC情報を複数銀行間で共有しない場合、必然的にプライベート型となり、ブロックチェーン／分散型台帳の特長である情報の共有化というメリットを活かせない。

においては現在の仕組みを踏襲できる可能性があり、導入に伴う影響は比較的少なく抑えられる可能性がある。

顧客企業と口座情報の共有を可能にすると、顧客企業とのダイレクトな台帳の連携が可能となる。例えば、顧客企業と口座情報を分散台帳で共有すると、顧客企業が自社の会計処理等で行う入金や出金の操作が、金融機関に対する入金や出金の指図を経ることなく共有され口座情報に反映されるようになる。

## ② 留意点・課題

既存システムにブロックチェーン／分散型台帳を適用する場合、(暗号化を含む)高いセキュリティを担保しつつ、現在と同程度の性能水準を維持することが求められる。現段階での技術水準では、中堅・大手行レベルで実用に耐え得る処理速度とセキュリティ水準の確保が難しい状況であり、技術革新が必要となる。

勘定系システムは、銀行システムの中心的な機能となることから、ブロックチェーン技術／DLTを活用する場合、周辺システムとの接続についても検証することが必要となる。また、既存システムが保有する大量の過去データについてブロックチェーン／分散型台帳の管理対象とする場合、移行方法やデータの持ち方についても併せて検討が必要となる。

### 4.2.4 金融インフラ

#### ① 活用可能性に関する考察

現在、銀行間で利用されている集中管理型の金融インフラをブロックチェーン技術／DLTで代替するかたちでの活用については、一般に、巨額の投資と長い期間を要するとされる<sup>34</sup>。他方、金融インフラでは、高い信頼性と安定性が求められるため、集中管理型システムではバックアップサイトの設置を含めて、大きな投資を必要としており、性能要件の低下に留意しつつ、ブロックチェーン／分散型台帳の特長である高可用性を活かし、ゼロ・ダウンタイムが実現できれば、コスト削減等が可能となる可能性がある。

ブロックチェーン技術／DLTの特長や限界を踏まえつつ、特定の業務やシステムについて、部分的な移行も選択肢となり得ると考えられる。

#### ② 留意点・課題

現在、銀行間で利用されている集中管理型の金融インフラでは、大量の取引を高速で処理している。一方、ブロックチェーン技術／DLTは、一般に、こうした種類

---

<sup>34</sup> World Economic Forum “The future of financial infrastructure”(2016)

の取引に不向きとされ、ブロックチェーン／分散型台帳によって代替する場合は、他の機能要件を充足しつつ同等の性能要件をいかに確保するかの技術的な課題をクリアする必要がある。

## 【BOX2】全銀システムへの応用可能性

### 1. 全銀システム（全国銀行データ通信システム）について

- ・ 全銀システムは、金融機関間の内国為替取引（国内における他行宛振込等）をオンライン・リアルタイムで処理するセントラルシステムで、一般社団法人全国銀行資金決済ネットワーク（全銀ネット）が管理、運営を行っている。全国の金融機関<sup>35</sup>とネットワークで相互に接続されており、全国の金融機関で受け付けられた顧客からの振込依頼は、全銀システムを通じてオンライン・リアルタイムに金融機関間で送受信され、受取人の口座へのリアルタイム着金を実現している。
- ・ 現在振込に係る為替通知等のデータは、全銀システムのテレ為替または新ファイル転送により送信されている。テレ為替は、振込等の為替通知のデータを1件ごとにオンライン・リアルタイムに発受信する仕組みで、500万件／時間（毎秒単位に単純計算すると、約1,389件／秒）、2,500万件／日の処理能力を有している。新ファイル転送は、株式配当金振込等、特定の日にまとめて振り込む為替通知のデータを一括して発受信するもので、2,600万件／日の処理能力を有する。

### 2. 今後の全銀ネットの取組方針

- ・ 現段階では、全銀システムへのブロックチェーン技術／DLTの活用には、性能要件を含む技術的課題があるものの、全銀ネットでは、以下の観点を持ちながらブロックチェーン技術／DLTの活用について検討を継続する方針としている。
  - ブロックチェーン技術／DLTの活用を検討する際には、既存システムの単純な置換えよりも、新たな仕組みとして検討することが有用と考えられる。
  - 全銀システムは大口／小口とも正確かつ高速に処理可能な資金決済システムとなっており、ブロックチェーン技術／DLTの活用に当たっては、こうした既存のサービスに対する利用者の期待や信頼に配慮しつつ慎重に検討する必要がある。
  - 接続する加盟銀行のシステム等へのインパクト（コスト面を含む）。
  - BISのFMI原則や金融庁「清算・振替機関等向けの総合的な監督指針」で求められる

<sup>35</sup> 現在、全銀システムに参加する金融機関は銀行のほか、信金、信組、労金、農協を含む1,296行（平成28年12月末現在）となっており、国内の預金取扱金融機関のほぼすべてがこのシステムを活用している。

資金清算機関の業務態勢の遵守について配慮する。

- 今後、ブロックチェーン技術／DLT等を活用した新たな送金サービスの登場が見込まれるなかで、決済インフラとしての役割・立ち位置の継続的な検証。

### 【BOX3】でんさいネットシステムへの応用可能性

#### 1. でんさいネット（全銀電子債権ネットワーク）システムについて

- ・ でんさいネットシステムは、電子債権の記録機関としての役割を担っている。記録原簿を備え、利用者の請求にもとづき電子記録や債権内容の開示を行うこと等を主業務とする。運営主体である全銀電子債権ネットワーク（でんさいネット）は、主務大臣（内閣総理大臣および法務大臣）の指定を受けた専門の株式会社として業務を行っている。
- ・ 現段階の性能要件等は以下のとおり（2016年12月末時点）
  - (1) 利用者数：約44万4千社／約59万9千契約
  - (2) 参加金融機関数：609<sup>36</sup>
  - (3) 共同中継センター数：3
  - (4) 運転時間（オンライン取引）：7:00～24:00<sup>37</sup>
  - (5) 性能目標<sup>38</sup>（オンライン取引）：更新系業務：3秒、参照系業務：1秒
  - (6) 業務データ保存領域：約5TB<sup>39</sup>

#### 2. 今後のでんさいネットの取組方針

- ・ でんさいネットシステムにブロックチェーン技術／DLTを応用するうえでは、例えば以下が論点となる。
  - 利用者、でんさいネット、参加金融機関それぞれにどのようなベネフィット、インセンティブがあるか検証が必要である。
  - 暗号化も含め、秘匿性をどのような実装で実現するか。システム設計、暗号化技術上の課題をクリアすると同時に、その実装が現行法令をクリアしているか等の法的課題にも配慮が必要となる。
  - ブロックチェーン／分散型台帳でシステム構成した場合、各金融機関のソフトウェア、ハードウェアの保守・運用の費用分担、責任分界をどう考えるかを検討する必要

<sup>36</sup> 内訳は、都銀/信託銀行：7、地銀/第二地銀：105、信金：265、信組：105、JA/信連/農中：123、その他：4。

<sup>37</sup> 毎月第2土曜日を計画停止日とする。なお、業務時間は、コアタイム（平日9:00～15:00）以外については参加金融機関の任意になっている。

<sup>38</sup> 50件/秒のオンライン請求がある場合を最大負荷想定とした性能目標値。

<sup>39</sup> 主要ディスク装置の記憶容量。でんさいネットシステム総体の記憶容量ではない。

がある。

- でんさいネットの取引においては「記録の訂正」が起り得るため、ブロックチェーン／分散型台帳の特長である「高改竄耐性」は制約になる可能性があり、対策の検討が必要となる。
- ブロックチェーン／分散型台帳上に記録可能な情報の形式と、現行のでんさいネットシステムが保有する過去データの形式は、必ずしも同一にできない可能性があり（前掲脚注 29 参照）、データの移行方法やデータの保有方法の検討が必要になる。
- 現行の電子記録債権法上、記録原簿への記録が債権の効力発生要件とされており、分散型台帳における記録原簿の考え方の整理が必要となる。このように、でんさいネットの運営、サービス提供は、電子記録債権法をはじめ、個人情報保護法、犯罪収益移転防止法等の関係法令にもとづき行われているため、関係法令への適合性、法令改正の要否について広範な検証が必要となる。
- でんさいネットの第2次中期事業計画（平成29年度～平成31年度）においては、まずは「全銀協の『ブロックチェーン技術の活用可能性と課題に関する研究会』での議論等も踏まえ、でんさいネットシステムにおけるブロックチェーン技術／DLT等の利用可能性やそのメリット・デメリット、利用に当たっての課題や影響等について検証」し、インフラコスト削減の可能性を見極めつつ、「システムの抜本的効率化を目指した取組みを進めていく」方針としている。

#### 4.2.5 その他

本稿で採り上げたユースケース以外にも、個別行レベルではさまざまなブロックチェーン技術／DLTの活用可能性に関する調査・研究、取組みが行われている<sup>40</sup>。加えて、近年では、みずほフィナンシャルグループ、三菱UFJフィナンシャル・グループ、三井住友銀行とデロイトトーマツグループによる国内の銀行間振込業務に関する共同実証実験や、SBI Ripple Asiaと国内銀行による内外為替一元化コンソーシアム等、銀行間で連携した取組みも拡がりつつある。

<sup>40</sup> 「3.2 個別の取組概要」を参照。

## 5. ブロックチェーン技術／DLTが銀行業務に変革をもたらす可能性を見据えて

### 5.1 官民挙げた取組みの必要性

ブロックチェーン技術／DLTは、銀行の業務やシステムに将来的に大きな変革をもたらす可能性のある技術である。わが国銀行界でも、現在、多くの銀行において、実証実験をはじめとする様々な活用可能性の検証・検討が行われている。

他方、銀行のシステムでは、高い安定性、信頼性、正確性が求められ、同技術の活用・実用化には、現状、技術面のほか、運用面、セキュリティ面や法制度面等、様々な点についてさらなる検討が必要となる。また、ビジネスルールや運用によってこうした課題の解決を図る場合、関係者が連携して対応していくことが必要になる。

ブロックチェーン技術／DLTの「分散型台帳」という特性や、銀行業務には銀行間ネットワークを前提とする取引、業務が多いこと、共通化することでコスト削減が可能な業務が存在すること等を踏まえれば、これらの課題の解決に向けては、個別銀行ベースの競争的な取組みに加え、官民の関係者の連携した取組みも同時に進めていくことが重要である。

こうした観点から、当検討会は、官民の関係者に対し、以下の取組みを提言する。

### 5.2 検討会提言（「ブロックチェーン官民連携イニシアティブ」）

#### 5.2.1 銀行界における「ブロックチェーン連携プラットフォーム」（仮称）の整備

現在、個別行レベルではブロックチェーン技術／DLTの活用可能性を検証すべく様々な実証実験が行われているが、「分散型台帳」というブロックチェーン技術／DLTの利点・特長を踏まえれば、こうした個別分野に加え、銀行間ネットワークを視野に入れた新たなサービスの開発や、コスト削減を目的とした非競争的な業務・システムの共通化等は、将来的に同技術の活用が期待される有力な分野である。

足許、ブロックチェーン技術／DLTの活用可能性の検討が、個別行レベルでのプライベート型から、銀行間で連携・協働したコンソーシアム型の検討フェーズに移りつつあることを踏まえれば<sup>41</sup>、こうした取組みを後押しする観点から、銀行界を

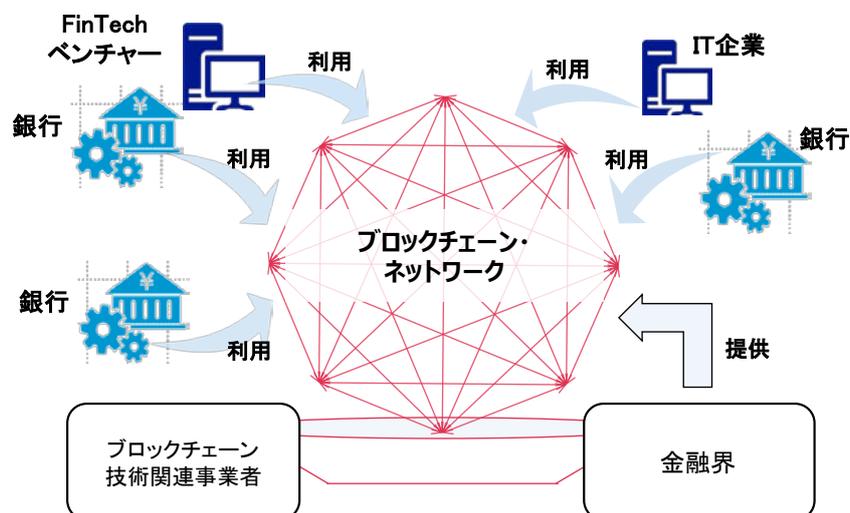
<sup>41</sup> 一般に、個別行レベルでの同技術の活用はプライベート型ブロックチェーン、銀行間で連携・協働した同技術の活用にはコンソーシアム型ブロックチェーンを前提として検討が行われる。

中心に、実用化に向けた連携・協働の容易化および開発コストの低減等を目的に、連携・協働型の実証実験環境として「ブロックチェーン連携プラットフォーム」（仮称）の来年度中を目途とした整備に向けた検討を進めることが期待される<sup>42</sup>。

「ブロックチェーン連携プラットフォーム」（仮称）においては、

- ✓ 銀行界がブロックチェーン技術関連事業者等と連携することにより、実証実験環境や情報連携の枠組み（ブロックチェーン・ネットワーク）を整備
- ✓ 当該枠組みの下で、IT 事業者や FinTech ベンチャー、事業者等と銀行が協働・連携して、ブロックチェーン技術を活用した金融サービス等の開発に向けた試行・実証実験を行うことを可能とする

【図表 9】 ブロックチェーン連携プラットフォームのイメージ



(注) 詳細は、今後、銀行界等において検討。

こうした環境整備を行うことにより、例えば、新たな決済・送金サービスや KYC、金融インフラ（全銀システム、でんさいネットシステム等）等、ブロックチェーン技術／DLT の活用が期待される分野について、実用化に向けた積極的な検討が進められることが期待される。

### 5.2.2 国際的な標準規格への対応戦略

ブロックチェーン／分散型台帳の基盤には、現在、様々な規格が存在しており<sup>43</sup>、

<sup>42</sup> ブロックチェーン技術／DLT の実用化に向けては、技術面の検証のみならず、法制度や安全対策基準の適用関係等、法制度面の課題解決が不可欠であることに鑑みれば、実証実験・検証には、法令等の適用関係の整理について関係当局の積極的な支援も期待される。詳細については、「5.2.4 ブロックチェーン技術／DLT の活用に向けた関係当局との連携」を参照。

<sup>43</sup> 主なブロックチェーン・分散型台帳基盤の概要は巻末参考資料をご参照。

あるブロックチェーン／分散型台帳の基盤を前提にプログラムされたアプリケーションは、原則として、他の規格の基盤では動作しない。したがって、将来的に海外金融機関との連携・協働も視野に入れた新たなサービスや仕組み等を検討するに当たっては、目的に応じて、国際的な普及可能性等を考慮したブロックチェーン／分散型台帳の基盤の選択が重要となる。こうしたブロックチェーン／分散型台帳の基盤を選択することは、ユーザーとして、仕様等の決定・変更に対する国際的な発言権を確保することにも資することになる。

銀行界における「ブロックチェーン連携プラットフォーム」（仮称）の整備に向けては、こうした国際的な標準規格を巡る動向や各基盤の特徴にも留意しつつ、相応しいブロックチェーン／分散型台帳の基盤を選定・検討のうえ、取組みを先進的に進めていくことが期待される。

### 5.2.3 金融インフラにおける活用可能性の検討

金融インフラへのブロックチェーン技術／DLTの活用については、技術的な面のみならず、インフラとしての安全性、安定性、信頼性、また、接続する銀行への影響等、様々な要素を多角的に考慮する必要があるが、将来的なインフラの改善やコスト低減等の可能性を見据え、先取的に活用可能性の検討をスケジュール感をもって進めていくことが重要である。

でんさいネットの第2次中期事業計画(平成29年度～平成31年度)においては、「全銀協の『ブロックチェーン技術の活用可能性と課題に関する研究会』での議論等も踏まえ、でんさいネットシステムにおけるブロックチェーン技術等の利用可能性やそのメリット・デメリット、利用に当たっての課題や影響等について検証」し、インフラコスト削減の可能性を見極めつつ、「システムの抜本的効率化を目指した取組みを進めていく」とされている<sup>44</sup>。でんさいネットにおいては、「ブロックチェーン連携プラットフォーム」（仮称）における実証実験も視野に、上記取組みを進めていくことが期待される。

また、全銀システムを管理、運営している全銀ネットにおいても、ブロックチェーン技術／DLTの活用について継続的に検討を行っていくこととされている。

今後、ブロックチェーン技術／DLT等を活用した新たなサービスの登場が見込まれるなかで、将来的な金融インフラとしての役割・立ち位置等も見据えつつ、各金融インフラ運営機関においては、これらの取組みを遅滞なく果敢に進めていくこと

---

<sup>44</sup> なお、電子記録債権取引にブロックチェーン技術を活用する場合、現行の電子記録債権法との関係についての整理に向けては、関係当局の支援も期待される。

が期待される<sup>45</sup>。

#### 5.2.4 ブロックチェーン技術／DLT の活用に向けた関係当局との連携

実用化を目指した実証実験を行う場合や、実験的に顧客等に利用してもらいフィードバックを得ながら課題等の洗い出しを進める場合、開発するプログラムや仕組み、ビジネスルール等は、最終的な法制度への準拠も視野に検討を進めていく必要がある。

他方、「フィンテックは、金融サービスを提供する基盤となる技術の革新を出発点として、新たなアイデアを実現しようとするものであるため、既存の制度の延長線上では整理をつけにくいことが多い<sup>46</sup>との指摘もある。また、ブロックチェーン技術／DLT の活用に向けては、様々な法的論点が存在する<sup>47</sup>。

関係当局においては、個々の実証実験や実用化に向けた検討における法制度面の論点整理について積極的に支援すること等を通じて、ブロックチェーン技術／DLT の実用化に向けた民間の取組みを後押ししていくことが期待される。

#### 5.2.5 ブロックチェーン技術／DLT の活用に向けた中央銀行との連携

金融インフラにおける活用可能性の検討を図っていくうえでは、中央銀行との連携を図っていくことも重要である。

中央銀行においては、決済の安全性確保や効率性向上等の視点を踏まえ、金融インフラ等へのブロックチェーン技術／DLT の活用の取組みについて、銀行界等と対話していくことが期待される。また、そうした取組みを国際的な決済を巡る議論との整合性を確保しつつ進めていく観点から、ブロックチェーンを巡る国際的な議論の動向等を銀行界等に随時還元していくことが期待される。

#### 5.2.6 安全対策基準の適用関係に関する整理

ブロックチェーン技術／DLT のユースケースにおいては、金融機関に生じる安全対策上の責任の程度が様々であることが想定される。FISC が策定する安全対策基準は、金融機関に安全対策上の責任が生じていることが前提となることから、個々のユースケースにおいて、個別金融機関に安全対策上の責任がどの程度生じているかを見極めることが重要である。また、ユースケースにおいては、安全対策基準が主たる前提としていなかったテクノロジー等が新たに採用されることも想定される。

<sup>45</sup> 新たなサービスの可能性やコスト低減の可能性が見込まれる場合には、「ブロックチェーン連携プラットフォーム」（仮称）において実証実験を行うこと等の取組みも考えられる。

<sup>46</sup> 木下信行「レギュラトリー・サンドボックスについて」（NBL 2017.1.15, p35）。

<sup>47</sup> 詳細については、末尾【参考資料 2】をご参照。

情報セキュリティ関連機関においては、安全対策上の責任面および技術面から、実証実験の動向やユースケースの出現状況等をにらみながら、ブロックチェーン技術／DLTに係る調査・研究を進めるとともに、改訂が予定されている新たな安全対策基準を前提として、その適用関係（解釈・運用等）を整理することが期待される。

### 5.2.7 ブロックチェーン・コミュニティの形成

ブロックチェーン技術／DLTは、現在、様々な関係者において、技術的な面も含めた課題解決や様々なユースケースへの応用に向けた検討が進められており、本報告書において言及した活用可能性や課題は、あくまで現時点での整理にもとづくものである。また、今後、実証実験等を通じて、新たな活用可能性や課題等が明らかになる可能性もある。

このため、IT事業者、ブロックチェーン関係団体／事業者、学者・研究者、関係当局等の幅広い関係者に、銀行分野における活用上の課題について理解を促し、課題解決、実用化に向けたさらなる研究や開発等を促していく必要がある。

こうした観点から、個別行において最新技術動向等を独自に調査・把握していくことに加え、銀行界においては、銀行間の連携・協働した実証実験を後押ししていくとともに<sup>48</sup>、実証実験を通じて得られた研究成果の概略<sup>49</sup>や幅広い関係者等からの技術動向等に関する情報提供について業界全体でシェアする枠組み等の整備等を通じて、コミュニティ形成を促していく取組みが期待される。

また、ブロックチェーン技術／DLTに関する科学研究（例えば、技術的研究、制度設計の研究、経済学的研究、等）が現段階では不足している状況のなか、健全かつ適切なカタチでの実用化に向けては、学術研究の分野においても、さらなる研究の推進と研究成果の共有、本分野の研究者の育成等が積極的に進められることが期待される。

以 上

---

<sup>48</sup> 例えば、実証実験主催銀行が業界団体を通じて、広く共同実験等への参画を募集できる仕組みを整備すること等が考えられる。

<sup>49</sup> なお、意義のある研究成果を得るうえでは、実証実験を行うに際してその目的や意義を明確にし、それに則した実証実験を企画・デザインすることが重要である。

## 【参考資料 1】主なブロックチェーン／分散型台帳基盤および関連技術の概要

既に実装事例や実証実験での使用事例があるブロックチェーン／分散型台帳基盤 8 種類を以下に紹介する。

### 1. Bitcoin Core

- ・開発元：Bitcoin Core (<https://bitcoin.org/>)
- ・特徴：Bitcoin のリファレンス実装。ブロックチェーン技術を最初に適用し普及した基盤。

### 2. Ethereum

- ・開発元：Ethereum Foundation (<https://www.ethereum.org/>)
- ・特徴：分散型アプリケーション (DApps) の構築プラットフォーム。専用プログラミング言語でコントラクトを記述可能。柔軟性があり様々な分野の実証実験に利用されている。

### 3. Hyperledger Fabric

- ・開発元：Hyperledger Project (<https://www.hyperledger.org/community/projects>)
- ・特徴：Linux Foundation が主導する Hyperledger Project で、オープン・ガバナンスの下、グローバル・スタンダードを目指して、開発が進められている P2P 分散型台帳技術基盤の一つ。Ver.0.7 では、コンセンサスアルゴリズムに PBFT が採用されている。

### 4. Corda

- ・開発元：R3 (<https://www.corda.net/>)
- ・特徴：R3 コンソーシアム主導で開発された金融業向け分散型台帳基盤。合意形成に焦点を当て、参加者全員で全データを共有しないことが特徴。2016 年 11 月にオープンソース化。

### 5. Chain Core Developer(Enterprise) Edition

- ・開発元：Chain (<https://chain.com/>)
- ・特徴：短時間で取引完了状態を実現してデータの一貫性を確保できる Simplified BFT という新しいコンセンサスアルゴリズムや、ブロックチェーンの暗号化等、企業利用を前提とした機能を備えている。

### 6. NEM

- ・開発元：NEM.IO Foundation (<https://www.nem.io/>)
- ・特徴：独自通貨機能を持つブロックチェーン基盤。コンセンサスアルゴリズムに PoI を採用。1 分間隔でブロック生成者がネットワークの貢献度に従い決定される方法により、省電力と参入障壁の低下といった効果をもたらしている。機能的にはマルチシグ、暗号化メッセージ等の機能や、効率的な運用・保守のために、ノードの評価システム等を搭載している。また NEM をベースに開発された、コンセンサスアルゴリズムに PoS を採用するクローズ志向の基盤として、mijin がある。

### 7. Orb 1

- ・開発元：Orb (<https://imagine-orb.com/>)
- ・特徴：運営主体により権威付けられた「スーパーピア」の存在により、中央集権型と分散型のメリットを融合。定期的に取り引を確定させることで、決済のファイナリティを確保。

### 8. Interledger (ILP)

- ・開発元：Ripple (<https://interledger.org/>)
- ・特徴：金融機関が保有する既存の台帳間を接続し、暗号化されたエスクローの仕組みを提供。中間業者を挟まずに 1 対 1 でやり取りするため、高速かつ安価に支払いが可能。ILP 自体は通信プロトコルの規格であり、全体で一つの台帳 (ブロックチェーン) や独自通貨を持たない。なお、コンセンサス部分は一般に開示されていない。

【図表 10】 代表的なブロックチェーン基盤／分散型台帳基盤の比較

	Bitcoin Core	Ethereum	Hyperledger Fabric
分類	パブリック、 コンソーシアム、 プライベート	パブリック、 コンソーシアム、 プライベート	コンソーシアム、 プライベート
コンセンサス アルゴリズム	PoW	PoW (2017年3月現在)	PBFT (2017年3月現在)
ファイナリティ	無し 各ノードがブロックを 作るため、ブロックチェ ーンが分岐した場合、一 度確定したトランザク ションが覆る可能性有 り	無し 各ノードがブロックを 作るため、ブロックチェ ーンが分岐した場合、一 度確定したトランザク ションが覆る可能性有 り	有り 更新時にコンセンサス をとって確定するため、 ファイナリティが存在
性能	ブロック生成の間隔は 10分単位、確定されたと 判断できるまでに1時 間程度要する	ブロック生成の間隔は 12秒単位、確定されたと 判断できるまでに数分 程度要する	更新時にコンセンサス をとって確定するため 高性能。(15ノードに つき10万TPSが目標)
アカウント管理	参加者は各ノードで管 理され、共有されないた め、参加者の流入を制限 する機能は無し	参加者は各ノードで管 理され、共有されないた め、参加者の流入を制限 する機能は無し	メンバシップサービス がユーザーとノードを 登録し、PKIベースの証 明書発行も行う
最小構成台数	1台から動作。1台の故 障に耐えるために2台 必要	1台から動作。1台の故 障に耐えるために2台 必要	PBFTで1台の故障に耐 えるために最低4台必 要
データ格納方法	取引情報をブロックチ ェーンに格納して伝播	ブロックチェーンにコ ントラクト自体も格納 して伝播	ブロックチェーンとワ ールドステートで構成
情報の秘匿化	無し トランザクションの内 容は一般公開	無し トランザクションの内 容は一般公開	有り 個々のトランザクショ ンに対し証明書を発行 し暗号化
スマート コントラクト 開発	Script 言語により実行。 シンプルな言語のため ループ処理や分岐構文 に制限有り、また拡張性 に乏しい <sup>50</sup>	Solidity という専用言語 でコントラクトと呼ば れるプログラムを開 発 <sup>51</sup>	Go と Java 言語により チェーンコードという プログラムを開発。今 後、Java Script を追加 予定。ソースからネイ ティブコードを生成して 直接実行。Docker コン テナの中で実行

<sup>50</sup> Bitcoin Core のスマートコントラクト開発における制限は、安全性や検証容易性を目的としている面もある。

<sup>51</sup> ソースコードは Ethereum Virtual Machine (EVM) と呼ばれる仮想マシン上で動作するため、プラットフォームに依存しない。Gas という一種の燃料の概念にもとづき、一定の処理コストの中で動作させる必要がある。

**【参考資料2】法制度面の論点**  
**片岡メンバー（片岡総合法律事務所所長弁護士）提出資料の概要**

ブロックチェーンに関する法制度を検討する際には、法制度に私法と公法の区別があり、そして、そのそれぞれに多層的な法平面があることから、問題の所在を明確にした上で、どの法平面でどの問題を検討するのかを明確にする必要がある。

そこで、ブロックチェーンを金融取引等に利用する場合に、上記の観点から踏まえておくべき基本的な法律上の論点として、次のような諸点を考えることができる。

**1.1 ブロックチェーンの類型に関する前提問題**

ブロックチェーンに関する法制度を検討する際には、ブロックチェーンに様々な類型からみた様々な類型があることから、そのマトリックスを念頭に置き、その類型ごとに、かつ、法制度の平面ごとに問題を検討していく必要がある。

ブロックチェーンには、事実上及び法律上の観点からみて大きくは次のような類型がある。

**(1) 管理者の態様による類型**

- ① パブリック型（原則として）管理者のないもの
- ② コンソーシアム型 複数の管理者のあるもの
- ③ プライベート型 単一の管理者のあるもの

**(2) 記録訂正の態様による類型**

- ① 訂正不可型（原則として）記録を訂正することができないもの
- ② 訂正可能型 記録を訂正することができるもの<sup>52</sup>
  - ア. 移転訂正可能型 訂正対象の内容から訂正後の内容に移転する記録をするもの
  - イ. 抹消訂正可能型 訂正対象の内容を削除し訂正後の内容を記録するものこの中でも、訂正対象の内容が記録から消去されてしまうものと、削除の記録が残るものとの相違がありうる。

**(3) 法的効力の態様による類型**

ブロックチェーンのユースケースを考える場合、法的観点からは、記録が有する法律効果との関係について、次のような類型に分類することができる。

- ① 法の規定により、その記録自体が法律上の権利自体についての強い法律効果を生じるもの。例：電子記録債権の記録（法律による法律上の権利推定）
- ② 法の規定により、記録自体が法律上の権利自体についてのものではないが、法律上の

<sup>52</sup> 訂正可能なものをブロックチェーンと呼ぶかどうか、単に DLT (Distributed Ledger Technology=分散型台帳技術) というべきかはともかく、取引記録の訂正が必要とされるユースケースで、ブロックチェーンのブロック自体の訂正はできないとして、個別の取引記録の訂正をどのように工夫ないし応用して行うかという技術上の問題は別途検討する必要がある。

権利に関する一定の法律効果を生じるもの

例：不動産登記（公信力はないが、法律による対抗力があり、また、判例上、権利に関する法律上の推定はないが、権利移転事実に関する事実上の推定があるとされる。）

③ 記録自体が直接の法律効果を生じないもの

例：商業帳簿（訴訟上証拠となることはありうるが、直接法律上の効果が生じるわけではない。）

## 1.2 ブロックチェーンの類型別の法律関係

### (1) パブリック型

パブリック型の場合は、管理者が不在であり、コンピュータシステムとしてのアルゴリズムがあるのみであるから、原因関係上の法律関係は契約法理で規律することはできず、原因関係上の債権法の法定の債権債務関係である①事務管理、②不当利得、③不法行為の各法理で決することになる。また、④信義誠実の原則、⑤権利濫用、⑥公序良俗違反、⑦条理という一般法理の適用もありうる。

### (2) コンソーシアム型

コンソーシアム型については、コンソーシアムを組成する原始ボードメンバーの全部又は一部の間で、合同行為としての組合等の組織の「規約」を定めるのが通常であると考えられ、原始的又は後日にこれに参加する者があっても、この規約により、組織法及び民事実体契約として、その規約による契約法理で規律されることになる。

そして、コンソーシアムは、この参加事業者と利用者との間のブロックチェーンに係る基本的な民事実体法の法律関係を契約法理で規律する「約款」を定めるのが通常であると考えられる。そして、利用者相互間のブロックチェーンに係る民事実体法の法律関係も約款法理により契約法理で規律することも認められるものとする。

他方で、コンソーシアム型のブロックチェーンについて、不正行為を行う者に対する民事実体法の規律を定めて、これに法律効果を及ぼし得るかは問題であり、コンソーシアム型という私的なブロックチェーンにアクセスする者である以上約款に定めれば、信義誠実の原則を含む契約法理による規律を及ぶ可能性もあるが、今後の検討課題であろうか。

### (3) プライベート型

プライベート型については、管理者が単独であるから、管理者が定める「約款」により契約法理（改正民法案 548 条の 2 以下の「定型約款」の規定参照。なお、コンソーシアム型についても同様である。）によって、規律されるものと考えられる。なお、利用者相互間の関係についても、コンソーシアム型と同様であろう。

## 2. 金融取引の法的構造及び階層に関する前提問題

### (1) 有因と無因

金融取引の法律効果を考えるに際しては、原因取引の法律関係の影響を受ける有因のもの

のか、その影響を受けない無因のものかを区別する必要がある。無因の取引である場合に、原因関係上の抗弁<sup>53</sup>がある場合であっても、それは原因取引の当事者間で効力を有してその間で解決されるべきもので、金融取引の当事者間には原則として効力が及ばない。ただ、「犯罪利用預金口座に係る資金による被害回復分配配当金の支払等に関する法律」（いわゆる振り込め詐欺救済法）等、特別法による救済措置等は別論である。また、金融取引自体に錯誤等の瑕疵があつて、組戻し等が行われることがあるのも別論である。

### ① 原因取引

金融取引が行われる背景ないし原因には、物の売買や役務提供取引等の原因取引がある。ただ、金銭の貸付けは、金融取引ではあるが、それ自体が原因取引である。

### ② 有因取引

原因取引の決済手段で実質的に与信機能がある取引であっても、いわゆる販売信用に係る「包括信用購入あっせん」、「個別信用購入あっせん」は、割賦販売法の民事規定により、原因関係上の抗弁の対抗を受ける。

また、「ローン提携販売」及び原因行為と密接牽連性の認められるいわゆる「提携ローン」については、そのローン取引は金融取引というべきであるが、原因行為との密接牽連性から、同じく割賦販売法の民事規定により、原因関係上の抗弁の対抗を受ける。

これらは、有因の金融取引となる。

### ③ 無因取引

原因取引があり、その代金の送金又は取立てのため、為替手形若しくは小切手又は約束手形を振り出す行為は、法律上、原因関係からは無因のものとして構成されている。原因取引の代金の送金又は取立てのために、為替取引を行うことは一種の金融取引であるが、この金融取引は原因関係とは無因のものとして構成され、原因関係上の抗弁の対抗を受けない。

## (2) 為替取引にみる法的構造と階層

FinTech のユースケースとなりうる（我が国の内国）為替取引は、次のような法的構造と階層を持つ。

① 第1平面：「原因取引」

② 第2平面：送金人、仕向銀行、被仕向銀行、受取人間の「為替取引」（送金為替の場合）

<sup>53</sup> 要件事実論

法律上の権利及び法律効果は、観念的な概念であるから、一定の法律事実があることを認識し、その結果一定の法律効果の発生を認識するという  $P(f) \Rightarrow Q(e)$  の構造を持つ。そして、この  $P(f)$  を要件事実といい、この  $Q(e)$  を法律効果という。権利発生 of 要件事実 ( $f$ ) を請求原因 (事実) といい、この権利発生 of 法律効果を障害、消滅又は阻止する法律効果をもたらす要件事実 ( $f$ ) を抗弁 (事実) という。そして、その抗弁 of 法律効果の発生を障害、消滅又は阻止する要件事実を再抗弁といい、再々抗弁、再々々抗弁と続く。このように実体的原因関係は、法律的には限りなく覆滅しうる可能性が認識されている。なお、この要件事実には、別途時的要素も含まれる。

この平面では、送金人と仕向銀行、仕向銀行と被仕向銀行、被仕向銀行と受取人間の 3 つの法律関係がある<sup>54</sup>。

③ 第 3 平面：仕向銀行、資金清算業者、被仕向銀行間の「資金清算取引」（全銀システムによるマルチラテラルネットィングが行われ、仕向銀行及び被仕向銀行は、資金清算業者（一般社団法人全国銀行資金決済ネットワーク（全銀ネット））に対し、決済戻の債権又は債務を有することになる。）

④ 第 4 平面：仕向銀行、中央銀行、資金清算業者、被仕向銀行間の「資金決済」（仕向銀行及び被仕向銀行の資金清算業者（全銀ネット）に対する決済戻（債権又は債務）は、全銀ネットから中央銀行（日本銀行）に通知され、この三者の日銀当座預金で決済される。）

なお、これらの法律関係の各平面では、それぞれ前者が後者の「原因関係」になる関係となる。第 1 平面と第 2 平面との関係は、原則として無因である。第 2 平面と第 3 平面の間もネットィングが効力を生じる前は有因であると考えられるものの、ネットィングが効力を生じればその時点で無因となる（「金融機関が行う特定金融取引の一括清算に関する法律」（一括清算法）3 条参照。なお、この規定により、強行法規である倒産法からもネットィングは効力を持つこととなって、倒産管財人から否認されない。）。第 3 平面と第 4 平面の間は、全銀ネットの業務方法書 55 条以下に決済戻不払の規定があり、これに鑑みると無因であるものと考えられる。

### (3) ファイナリティの概念に関する問題

為替決済に関しては、ファイナリティが議論される。ただ、この概念は、①当事者間完了性、②対第三者完了性、③資金決済完了性、④支払指図の撤回不能性等、多義的に用いられるとされる<sup>55</sup>。

この問題は、上記(1)及び(2)の為替取引の構造とその有因無因とに関係するものと考えられる。そして、一定の当事者間での債権債務ないし貸借関係が消滅し、これがその法平面での法律関係が覆滅しないことをいうものと考えられる。したがって、第 2 平面での為替取引が完了すれば、たとえ第 1 平面での原因関係に法律行為の瑕疵等があっても無効、取消し等の問題が生じても、法平面間の法律関係は、無因であるから、第 1 の原因関係の平面での法律関係の処理がなされても、第 2 の為替取引の平面での法律関係は消滅しており、影響を与えない。

他方、各法平面間の法律関係が有因であれば、前述（42 頁注 53 要件事実論）したように、原因関係上の法律効果は、実体法的にはいかなる原因でいつ覆滅等するか分からず、その法律関係の判決が確定するまでは、有因の法律関係も確定しないということになる。

したがって、ファイナリティを法的に検討する際には、上記要件事実論に鑑みても、当事者、法平面、時的要素を特定して論じる必要がある。そして、その契約関係及び法律関係が無因のものとして構成されていればその関係でその法平面でファイナリティがあると

<sup>54</sup> 被仕向銀行と受取人の間には、為替取引上の法律関係はなく、受取人の被仕向銀行に対する請求権はないと解されている（判例）が、資金受取り等のために預金契約の法律関係があるのが通常であり、そうするときは、預金口座に入金された預金払戻請求権を有することになる。

<sup>55</sup> 嶋拓哉「資金決済におけるファイナリティ概念について—ファイナリティ概念の多義性を巡る法的検証」金融庁金融研究研修センター<http://www.fsa.go.jp/frtc/nenpou/2006a/11.pdf>

いべきものと考えられる。したがって、決済に関するシステムすなわち約定がいかにか構成されているかによっても影響を受ける。なお、国際的にも<sup>56</sup>国内的にも決済のファイナリティとして関心が高いのは、システムリスク回避の観点から、上述の第3及び第4平面での金融機関と資金清算業者及び中央銀行に関する関係であろう<sup>57</sup>。

したがって、ファイナリティは、その決済システムが各法平面での契約がいかにか構成されているかとの点や、契約以外の倒産法や物権法等に係る法律関係によって決せられることになる。

### 3.ユースケース別の法的論点に関する考察

#### 3.1 仮想通貨関係

##### (1) 仮想通貨の私法上の性質

我が国の民法等の私法は、「物」「人」「金銭」「物権」「債権」の概念を規定するのみであり、また、債権質や知的財産権のような「人」の「権利」に対する支配権である「準物権」の概念を規定するが、物権及び準物権については、物権法定主義により法定がなされないと法的な権利にはならない。仮想通貨にも、「人」の「財産的価値」についての事実上の支配という機能は認められるから、構造としては「準物権」に類似する。しかし、仮想通貨の財産的価値が「権利」といえない以上は、「準物権」ということもできない。ただ、準物権と同様の構造を有することから、物権法自体を適用することはできないが、一般法理によって、物権法に類する規範が適用されうる<sup>58</sup>。

そこで、仮想通貨自体に関し、何らの関係者の契約上の意思表示がない以上契約法理の適用はないが、仮想通貨を巡っては、前述のとおり、①事務管理、②不当利得、③不法行為の法定債権関係は生じうるし、一般法理の適用はありうる。

なお、原因関係取引があつて、その決済に仮想通貨を用いるような場合に、かかる原因関係取引の合意について契約法理の適用があるのは別論であるし、仮想通貨に関して取引をする場合も、その点に契約法理が適用されることも当然のことである。

ただ、仮想通貨自体の法律関係については、国際的なコンセンサスに基づく商慣習等が形成されるか、法制化が図られない限り、その私法関係は上記の一般法理に寄らざるを得ないものになるものと考えられる。仮想通貨を巡る様々な事象について、一般法理がどのように適用されることになるのかという点は、今後明らかにされてゆくべき今後の課題であると考えられる。

##### (2) 仮想通貨とブロックチェーン

仮想通貨は、極めて多くの種類が出現するに至っているが、Bitcoinが最も多く流通して

<sup>56</sup> 国際的には、ファイナリティに関し、BIS（国際決済銀行・決済・市場インフラ委員会）のFMI（Financial Market Infrastructure）原則がある（第8原則）。

<sup>57</sup> 我が国では、全銀ネットの業務方法書に基づく契約関係と一括清算法等の法律によって、資金清算業者である全銀ネットと参加金融機関相互間の法律関係であるファイナリティが決定、確保されることとなる。

<sup>58</sup> 森下哲朗「FinTech時代の金融法の在り方に関する序説的検討」企業法の進路（江頭憲治郎先生古稀記念）771頁以下、とくに807頁参照

おり、また、ブロックチェーンの技術は、Bitcoinによってもたらされたことから、ここでは仮想通貨のうちBitcoinについて考察する。

Bitcoinのブロックチェーンは、管理者がいないパブリック型であり、記録の訂正をすることができないタイプである。そして、ブロックチェーンにBitcoinの記録がなされれば、その保有者は暗号技術の秘密鍵の情報を持つことにより財産的価値を有する仮想通貨としてのBitcoinを事実上支配してこれを保有するという機能を有する。この点、法律が法律効果を規定しているのではなく事実上の機能にすぎないから、この点を強調すれば、前述の分類では何ら法的効果と結びつかない第3の類型ということになる。

他方、事実上の財産的価値を持つという資金決済法上の仮想通貨の要件を満たすものと考えられることから、少なくとも不法行為法上は法的保護がなされるものと解され、その限度では法律効果があり、前述の第1又は第2の類型に準じるものということもできる。

この点が財産的価値は認められるものの、私法上、物、金銭、物権、債権、準物権のいずれでもないという仮想通貨の特徴を示している。

### (3) 仮想通貨のファイナリティ

仮想通貨の移転のファイナリティについては、ブロックチェーンにfork（分岐）が生じる可能性がある以上、その平面で覆滅する可能性がない対第三者完了性や資金決済完了性に擬すべき仮想通貨移転完了性もないといわざるをえない<sup>59</sup>。

ただ、仮想通貨を取引代金の決済に用いる場合に、当事者間の約定で一定の事実又は時点をもって当事者間完了性はあったものとし、それが覆滅した場合の不都合について、原因関係の法平面で処理することとするはありうることも考えられよう。

## 3.2 電子記録債権

全国銀行協会が設立した電子債権記録機関である株式会社全銀電子債権ネットワーク（でんさいネット）がブロックチェーンの技術を用いてその業務を行う場合を検討する。

### ① ブロックチェーンのタイプと法律関係

でんさいネットにブロックチェーンを用いる場合には、検証に参加するノードを構成する金融機関が複数であることを想定する点で、コンソーシアム型が想定されている。ただし、電子記録債権法上、でんさいネットが指定電子債権記録機関としての主体であり、その位置付けを変更するものでない限りは、同社が法律上様々な義務を負うことから、法律上はプライベート型に準じる管理者としての権限を有することになる、この観点からは、でんさいネットが指定電子債権記録機関としての特権を持つこととなり、コンソーシアム型のブロックチェーンではあるものの、プライベート型との折衷的な形態となるものと考えられる。

そして、電子記録債権記録機関の業務自体が法定されており、電子記録債権については訂正の記録をするべきことが法定されているから、ブロックチェーンの記録も訂正可能な

<sup>59</sup> Bitcoinのブロックチェーンの場合には、ブロックが6個形成されたときに、数学的な見地から、forkが生じる可能性が著しく低いことから、事実上ファイナリティがあったと考えることが一般的であるとされている。しかし、覆滅される可能性自体は残る。

ものでなければならない。ただ、訂正記録の方法についての具体的な詳細は法定されておらず、当該指定電子債権記録機関の業務規程によることになる（同法 59 条、同法施行規則 25 条 1 号）。

そこで、業務規程にブロックチェーン使用に係る訂正の方法について規定をすれば、法改正まではしなくとも対応できるものと考えられる。ただ、ブロックチェーンの記録の訂正方法と電子記録債権法が求める訂正方法との整合性は求められることになる。

そして、電子記録債権の電子記録は、法定の場合を除き、そのまま権利発生及び譲渡等による権利移転等の取引の法律効果が発生することとされている。ただ、ブロックチェーン自体の各ノードの複数の電子記録をそのまま電子記録債権法上の電子記録とすることも考えられなくもないが、その記録と同期されている指定電子債権記録機関の特定の電子記録が同法上の電子記録であるとするのが現実的であるとも考えられる。

## ② 参加するノードの金融機関の守秘義務

でんさいネットのシステムが保有する電子記録債権に係る各種データは秘匿性が高い情報であるから、参加金融機関がノードとしてブロックチェーンの情報をどの範囲で保有することとするかは制度設計上の問題となる。

また、参加金融機関は、その情報につき守秘義務を負うべきこととなるが、法人顧客情報の守秘義務に関しては、全国銀行協会の貸出債権市場における情報開示に関する研究会報告書（平成 16（2004）年 4 月）<sup>60</sup>が参考になるものと考えられる。

さらに、債権者又は債務者その他電子記録に個人情報を含む場合には、電子記録債権を発生させるための当事者の請求の際に、個人たる当事者及び関係者の個人情報の第三者提供に関する同意（個人情報保護法 23 条）を取り付ける実務を行うことが考えられる。

## ③ 電子債権記録機関等の責任

でんさいネットにコンソーシアムプライベート折衷型のブロックチェーンを用いた場合も電子記録債権法上の電子債権記録機関の責任は、指定電子債権記録機関であるでんさいネットが負うものと考えられる。

コンソーシアムに参加する各ノードやボードメンバーとなる金融機関については、でんさいネットの業務規程に定めれば、これに基づく契約上の責任を負い得ることになるし、また、実務的には、かかる責任及び責任分担等に関する定めをすべきものと考えられる。

## ④ 電子記録債権についての強制執行

電子記録債権についての強制執行については、電子記録債権法等に規定があり（同法 49 条 3 項等、民事執行規則 150 条の 9 以下）、これとの整合性を図る必要がある。

この点については、電子記録の原本としてのノードをブロックチェーンと同期された指定電子債権記録機関のものであるとするときは、でんさいネットが民事執行法の当事者となり、特段の法律上の手当ては要しないものとも考えられる。

<sup>60</sup> <http://www.zenginkyo.or.jp/fileadmin/res/news/news160490-1.pdf>