【金融庁ブロックチェーン国際共同研究プロジェクト】

金融庁　御中

「金融セクターにおけるトークナイゼーションの進展とブロックチェーンのRegTech/SupTechへの活用可能性に関する研究」研究結果報告書

令和６年11月

株式会社クニエ

謝辞・免責事項

謝辞

- 本報告書作成にあたっては、京都大学・岩下直行教授、一橋大学・佐々木清隆教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。また、デジタル庁のオブザーバー及び金融庁のご担当者からも有益な示唆・助言をいただいた。
- もっとも、本報告書に関する内容の誤りは、すべて受託者である株式会社クニエに帰する。

免責事項

- 本報告書の内容は金融庁の公式見解を示すものではない。
- 本報告書で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性がある。

研究の目的・背景

- ブロックチェーン等の技術革新に伴い、金融サービスのデジタル化にとどまらず、決済手段や金融商品のトークナイゼーション（例：ステーブルコイン、トークン化預金、セキュリティトークン）等を通じて、一定のプログラマビリティを備えた金融システムが実現していく可能性がある。ブロックチェーンの最初のユースケースである暗号資産も含めて、これらの変化がもたらす機会とリスクの双方に配意しつつ、健全な金融システムの発展に向けて重要となる論点を特定し、分析を行っていくことが重要と考えられる。

- 銀行等の伝統的な金融機関も含め、国内外の多くの金融機関がブロックチェーンやトークナーゼーションの活用可能性を探っているところ、これらの技術がもつ自動化や自律性といった特性は、決済システムの効率化やコンプライアンス関連業務の自動化などを通じて金融システムの高度化に資する可能性を秘めている。他方、 P2P（個人間取引）やM2M（機械間取引）の増加といった潜在的な金融取引の様態の変化や、スマートコントラクトの脆弱性に起因する取引停止など、金融システムの安定や利用者保護、AML/CFT等の観点からリスクをもたらす可能性も指摘されている。

- 加えて、規制当局側もブロックチェーン関連技術を含むテクノロジーを最大限活用して、規制監督の高度化を図っていくべきとの指摘もある。例えば、FSBの報告書では、ブロックチェーンに限定した文脈ではないが、テクノロジーが「被規制金融機関や規制当局にチャンスとリスク、そして課題をもたらしている」と言及し、被規制金融機関によって利用される、規制・報告義務等の法令遵守をサポートするイノベーティブな技術（以下、RegTech）、規制当局によって利用される、規制業務を支援するイノベーティブな技術（以下、SupTech）のツールは、「金融の安定にとって、重要なメリットをもたらす可能性がある」と評している。

- 現時点ではトークナイゼーションの進展は限定的ではあるが、その将来における可能性に鑑み、トークナイゼーションの進展に伴う金融システムへのインプリケーションを分析するとともに、被規制金融機関および規制当局側がブロックチェーン技術等を活用したRegTech/SupTechにより規制監督対応を高度化させる可能性を分析することは重要と考えられる。

- 本調査研究では、第1章において、トークナイゼーションの進展を具体的事例や監督当局の対応も含めて概括する。第2章では、先行事例の分析等を通じてブロックチェーン技術等のRegTech/SupTechへの活用可能性を探る。第3章では、 RegTech/SupTechの１つのアプローチとされる「埋め込み型監督」および「監督ノード」に関する机上検証等を通じて、その可能性と課題について整理・分析を行う。

出典： FSB The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions
RegTech/SupTechの定義（経済産業省「『RegTech /SupTechに係る今後の在り方に関する検討会』について」）

目次

略語

本文書に登場する主な略語の正式名称を以下に示す。

略語	正式名称
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism マネー・ローンダリング及びテロ資金供与対策
BIS	Bank for International Settlements 国際決済銀行
DeFi	Decentralized Finance 分散型金融
FATF	Financial Action Task Force 金融活動作業部会
FSB	Financial Stability Board 金融安定理事会
KYC	Know Your Customer 顧客確認のプログラム
CBDC	Central Bank Digital Currency 中央銀行デジタル通貨
DAO	Decentralized Autonomous Organization 分散型自律組織
DLT	Distributed Ledger Technology 分散型台帳技術

用語集

本文書において、第１章に登場する主な専門的な用語について、以下のとおり定義する。

用語	定義
トークンナイゼーション（トークン化）	トークナイゼーションについて、金融安定理事会（FSB）は「資産のデジタルな表章（トークン）を作り出し、分散型台帳上に置くプロセス」と、国際決済銀行（BIS）は「金融資産や実物資産に関する権利を、プログラマブルなプラットフォームにおいて、デジタルに表章するプロセス」と定義している。 トークンナイゼーションの対象となるものは預金や金融商品、実物資産など多用であり、一例としてセキュリティトークン、ステーブルコイン、トークン化預金（Tokenized deposit）、NFTなどが含まれる。
ブロックチェーン関連技術	分散型台帳技術プラットフォームが必ずしもトークナイゼーションに利用されるとは限らないが、本報告書ではトークンナイゼーションに用いられる技術の総称として、「ブロックチェーン関連技術」という用語を使用する。
プログラマビリティ／プログラム化	プログラマビリティとは、一般に、ルールや条件をプログラムとして記述し、コンピュータに処理させることで、人手による作業を減らし、自動化と効率化を達成しうる性質のことを指す。北條氏・鳩貝氏 (2022)の報告書によると、例えば決済システムにおけるプログラマビリティとは、資金や証券が流通する際の振舞いをコンピュータプログラムによって制御し、自動化できる性質を意味する。金融セクターにおいては従前からプログラム化の取り組みがなされているが、本文書では、プログラム化をブロックチェーン関連技術を用いている場合に限定して用いる。
スマートコントラクト	ブロックチェーンに書き込まれ、トランザクションを通して機能が呼び出された際に自動的に実行されるルールを定めたプログラム なお、Ethereum等では、スマートコントラクトはブロックチェーンに書き込まれ、トランザクションの検証の過程でマイナーもしくはバリデータにより実行される。その実行ログと実行後の証憑がブロックに記録されることで、誰もが真正なプログラムコードが実行されたことを確認でき、また状態を共有できる。スマートコントラクトは通常は修正や削除ができず、実行結果は元に戻せないが、開発ツールによるサポート等を通して間接参照を用いれば、参照先を新たなコントラクトアドレスで置き換えることでスマートコントラクトをアップグレード可能にできる余地も存在する。スマートコントラクトはブロックチェーンにデプロイすることで実行可能になるが、DeFi におけるデプロイ作業は一般に管理者や権限者（スマートコントラクトのデプロイに必要な秘密鍵を保持している者）が保有する外部所有アカウントの秘密鍵が必要になる。
パーミッションレスチェーン	不特定多数の参加ノードがネットワーク上の取引を検証・承認する形態を取り、管理者の許可がなくても参加できる共有台帳。
パーミッションドチェーン	管理者に許可された特定のノードのみがネットワーク上の取引を検証・承認する形態を取り、参加者が限定的であるような共有台帳。

出典：Financial Stability Board (2023), ”The Financial Stability Risks of Decentralised Finance.”
Bank for International Settlements (2023), ”Blueprint for the future monetary system: improving the old, enabling the new.”
https://www.boj.or.jp/research/wps_rev/rev_2024/data/rev24j10.pdf

用語集

用語	定義
分散型金融（DeFi）	いわゆるDeFiについては、様々な文献や記事などで論じられているが明確な定義はされていない。当報告書では参考文献に従い「分散型金融システムの一部を構築する金融アプリケーション」と定義する。DeFiは、Ethereumブロックチェーンのローンチの後、当初は資金調達のための独自トークン発行や、トークンの交換に従来型の取引所の仲介を必要としないDEX（分散型取引所）が主であったが、DeFiエコシステムの拡大に伴い、レンディングやデリバティブ、保険など伝統的金融を踏まえて様々な取り組みが発生している。また、複数のDeFiの取引を1つにまとめてサービスを提供するアグリゲーターなどもある。
分散型金融システム	2019年のFSBの報告では、分散型金融システムを「分散型金融テクノロジーがもたらす可能性のあるシステム」と定義している。さらに、分散型金融テクノロジーを「金融サービスの提供における１つ以上の仲介者または集中型プロセスの必要性を削減または排除する可能性のあるテクノロジー」と定義している。当報告書においても上記の定義を用いる。 ※ 分散型金融システムは、既存の金融システムなどに見られる中央集権型（centralized)に対して非中央集権型(decentralized)のシステムの構築を目指しているとされる。本報告書において、「分散」は非中央化の意味を含んでいるとして用いることとする。
DAO	DeFiを運営する分散型自律組織（DAO）について、定まった定義は存在していないが、当報告書では、参考文献やMakerDAOの事例などを踏まえて、「中央集権的なリーダーシップが不在のメンバー所有のコミュニティで、コンピュータプログラムとしてエンコードされたルール（スマートコントラクト）によって運営が行われる組織」と定義する。 ※ 主なDeFiプロジェクトにおけるDAOの特徴 • 運営する会社や代表者・取締役会などが存在せず、参加者が自律的に運営を行う組織 • 組織の運営ルールがスマートコントラクトによってコード化されている • ガバナンストークンなどと呼称されるトークンに紐づく形で一種の議決権（投票権）がトークン保有者に付与され、組織・コミュニティの意思決定（の一部）について、スマートコントラクトのルールに基づいて投票が行われる • 複数の国に所属する参加者がグローバルに活動する組織であり、また必ずしも管理法人が明確でないため、組織が所属する国や地域の特定が困難

第１章　金融セクターにおけるトークナイゼーションの進展

１　ブロックチェーン関連技術と分散型金融システムの登場と普及

- ブロックチェーン関連技術と分散型金融システムに関する登場と普及の歴史を以下に示す。

1. ブロックチェーン技術の誕生

- 2008年: サトシ・ナカモトの名で知られる人物（またはグループ）が、「Bitcoin: A Peer-to-Peer Electronic Cash System」という論文を発表。この論文で初めてビットコイン（Bitcoin）という暗号資産とその基盤技術であるブロックチェーンの概念が紹介された。
- 2009年: ビットコインの最初のバージョンがリリースされた。これがブロックチェーン技術の誕生となる。

2. ビットコインの普及とブロックチェーン技術の進化

- 2010年: 初のビットコイン取引が行われ、2つのピザが10,000ビットコインで購入されたと言われている。これがビットコインによる初期の経済的取引事例とされている。
- 2011-2013年: ビットコインが徐々に広がり、他の暗号資産（アルトコイン）が登場。例えば、ライトコイン（Litecoin）やリップル（Ripple）などがある。
- 2015年: イーサリアム（Ethereum）が正式にリリース。イーサリアムは、スマートコントラクトを実行できるプラットフォームであり、暗号資産以外にブロックチェーン技術が応用された例である。

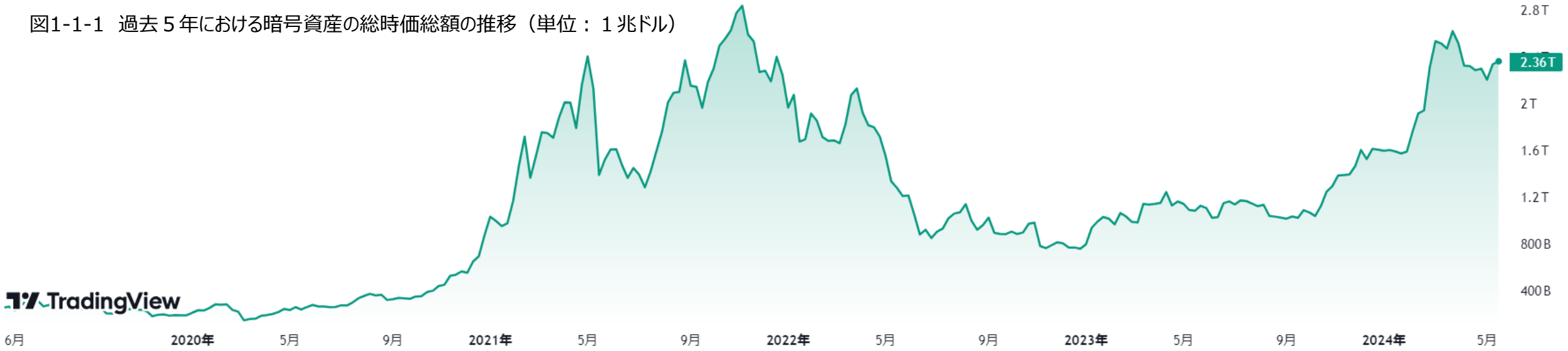
3. 分散型金融（DeFi）の台頭

- 2016年: The DAO事件が発生し、スマートコントラクトにおけるプログラムコードの脆弱性を付く攻撃のリスクなどの危険性が幅広く認識されはじめるものの、イニシャル・コイン・オファリング（ICO）により、多額の資金が調達され、多くのDeFiプロジェクトが開始される。
- 2018年: コンパウンド（Compound）やメイカーDAO（MakerDAO）などの初期のDeFiプロジェクトが現れる。USDCやDaiなどのステーブルコインが導入され、分散型金融取引が活発化した。このころ、国内最大規模の暗号資産流出事件が発生した。また、ICOに対する規制のあり方の議論が高まる。
- 2020年: いわゆる「DeFi Summer」と呼ばれる期間が到来し、分散型取引所（DEX）が急速に発展。ユニスワップ（Uniswap）やスシスワップ（SushiSwap）などが広がる。DeFiにおける総ロック価値（TVL: Total Value Locked）が急増した。

4. 最近の動向

- 2021年以降:クロスチェーン技術（異なるブロックチェーン間での相互運用性を実現する技術）の進展等もあり、DeFiエコシステムが更に複雑化。一方で、DeFiのハッキング被害も増加し、毎年多額の暗号資産が窃取されている。
- 2024年：2022年に下落した暗号資産の時価総額は回復しつつある。

図1-1-1　過去５年における暗号資産の総時価総額の推移（単位：１兆ドル）



出典：TradingView「暗号資産の総時価総額 — インデックスチャート」https://jp.tradingview.com/symbols/TOTAL/ 2024/5/20時点

２　分散型金融と伝統的金融の比較

（１）証券監督者国際機構（以下、IOSCO）報告書により指摘された分散型金融の規制に関する課題

- IOSCOによる「分散型金融に関する政策提言を含む最終報告書」（2023年12月公表）において、分散型金融の規制に関する課題を指摘している。（下記表を参照）

表1-2-1　IOSCO報告書における分散型金融の規制に関する課題

分散型金融の規制に関する課題	具体的内容
投資家保護を目的とした規制の必要性	• 近年、世界中の投資家が分散型金融にさらされる機会が増加しており、規制の不遵守、金融犯罪、詐欺、市場操作、マネー・ローンダリング、その他の違法な暗号資産市場活動の中で、投資家の損失も増加している。
分散型金融市場と伝統的金融市場の類似性をもとにした既存の規制枠組みの適用可能性	• 分散型金融市場と伝統的金融市場の経済的機能や活動が類似していることから、分散型金融の商品、サービス、活動、取り決めには、既存の国際的な政策、基準、管轄地域の規制枠組みが多く適用可能である。
分散型金融と伝統的金融市場に関するルールの適用・執行方法の違いから生じる規制裁定リスクの低減	• FSB、FATF、BIS などの国際機関間、および IOSCO、CPMI-IOSCO（Committee on Payments and Market Infrastructures-IOSCO）、BCBS（Basel Committee on Banking Supervision）などの基準設定機関間の 分散型金融 に関する協力と調整という広範な文脈において、IOSCO の勧告およびガイダンスは、暗号資産市場と伝統的金融市場との間の公平な競争の場を促進し、分散型金融と伝統的金融市場に関するルールの適用・執行方法の違いから生じる規制裁定リスクの低減に役立つはずである。
一貫した指導原則の必要性	• 暗号資産市場では、さまざまな取り決めに沿って、個人や事業体が金融商品を提供し、金融サービスを提供し、伝統的な金融市場と実質的に同じような金融活動に従事するのが一般的である。このような活動は、程度の差こそあれ、DLTを含む数多くの技術を使用して行われる。しかし、組織形態や使用される技術に関わらず、これらの人物や事業体は、"同じ活動、同じリスク、同じ規制・規制結果 "という指導原則に沿って扱われるべきである。

出典：IOSCO 分散型金融（DeFi）に関する政策提言を含む最終報告書 2023年12月

（２）分散型金融の特性

分散型金融の代表的特性には以下があると考えられる。

- 中央集権的ではない組織による運営が可能であること
- サービス提供者から身元を詮索されずに取引が可能となること
- 銀行口座が不要でネット環境さえあればグローバル規模で利用可能であること
- システム利用料が低いとされていること
- レンディングサービスや分散型取引所（ＤＥＸ）などの新機軸とみえる金融サービスがあること
- 暗号資産との親和性が高いこと

IOSCOの報告書において「金融商品・サービスの提供や提供、あるいは金融活動に従事するために使用される可能性のあるテクノロジーに関わらず、世界の市場規制当局が金融市場に対して『同じ活動、同じリスク、同じ規制・規制結果』のアプローチを適用すべき」とあるとおり、分散型金融は、金融システムの一種であるならば、システムの態様がどうであれ、金融規制の目的に沿った対応がなされているべきであると考えられる。他方、上記の特性のなかには、利用者保護やAML/CFTといった規制の目的を満たすことを難化させるものがあると考えられる。

以下に例示する。

- 中央集権的ではない組織による運営が可能であること　➡DAOによる運用の場合、事故等が発生した際に、責任の所在が不明瞭
- サービス提供者から身元を詮索されずに取引が可能となること　➡脱税やマネー・ローンダリングなど、犯罪の温床
- 銀行口座が不要でネット環境さえあればグローバル規模で利用可能であること　➡脱税やマネー・ローンダリングなど、犯罪の温床
- システム利用料が低いとされていること　➡金融規制趣旨に沿った対応が不十分なため、規制対応コストが利用料に含まれていない

出典：IOSCO 分散型金融（DeFi）に関する政策提言を含む最終報告書 2023年12月

（３）初期の分散型金融と伝統的金融の特性の比較

伝統的金融では、取引主体はKYC済であり、主なサービス提供者は業規制のもと、認可を受けた金融機関が担っており、当局等により、監督下に置かれている。伝統的金融に対する監督のあり方としては業規制による認可、自主規制、当局等からの利用者保護や金融市場安定化を目的とした監督対応など、幾重もの仕組みがあり、これらを信用の根拠として、利用者にサービス提供している。

分散型金融 (とくに誕生初期) では、取引主体は不明瞭であり、主なサービス提供者はこちらも主体が不明瞭なDAOである。分散型金融の多くでは、管理する第三者を排除する試みが見られるが、その上で秩序を維持しようとするならば、暗号学的技術を用いたプロトコルに全員が従うことを前提に、参加者が相互に監視し合うことをもって自己監督することになる。(表1-2-2 参照)

表1-2-2　伝統的金融と分散型金融の比較

	サービス提供者	取引主体	信用の根拠
伝統的金融	法人	KYC済みの個人・法人	自主規制、業規制、当局等からの監督
（当初の）分散型金融	DAO	KYC未済の個人・法人	暗号学的技術、参加者による相互監視

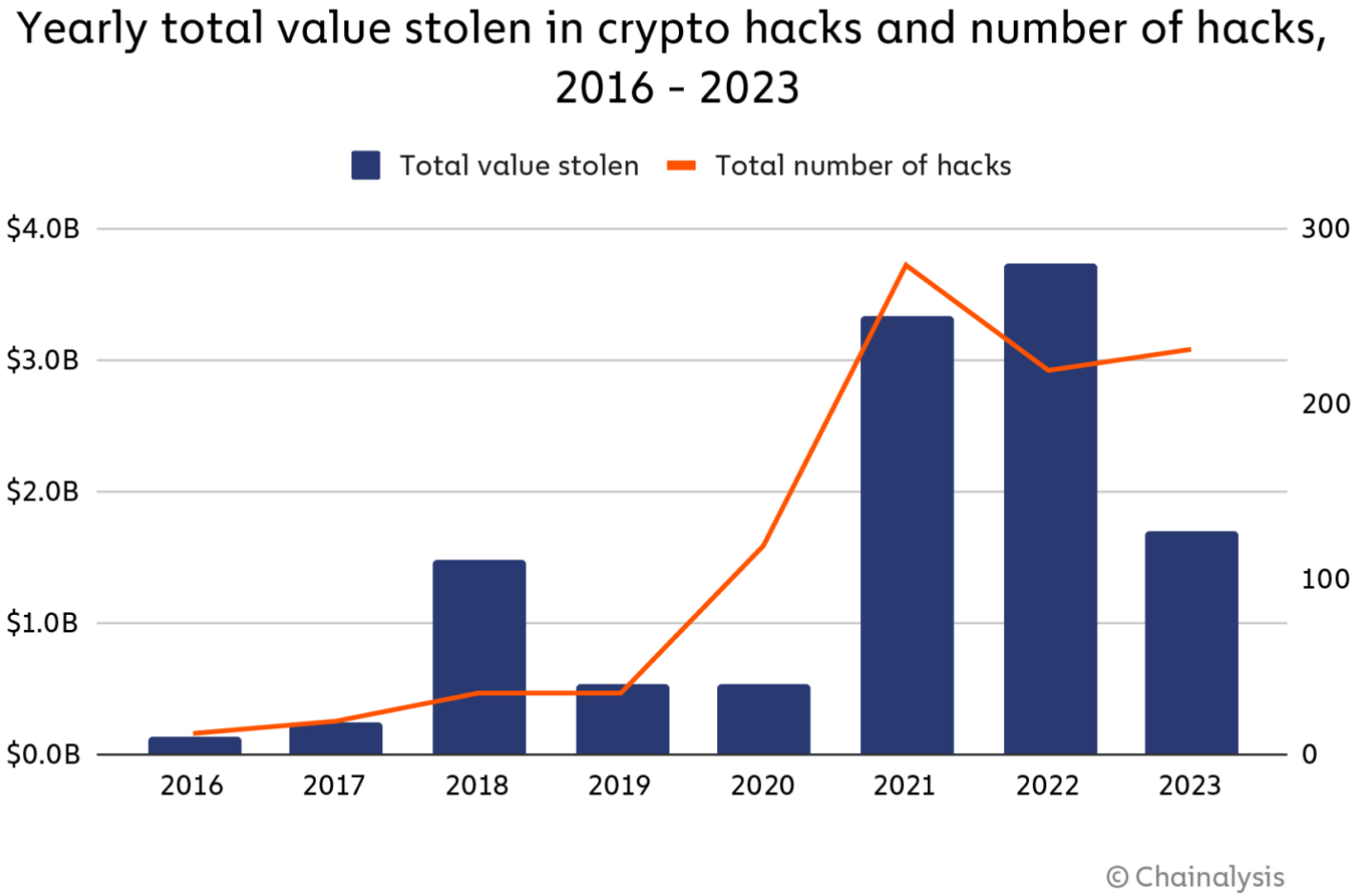
相互監視や自己監督について、以下に補足する。

分散型金融はグローバルな実体であるので、特定の国や地域の法に従わせることが困難である。一方で、参加者にはそれぞれが所属する国や地域の法の遵守が求められる。そこで、分散型金融では、プロトコルに従わないトランザクションやブロックを排除する前提のもとで、例えば参加者が送金を行う際に、関わると罰せられるような送金先でないかどうかを自身で確認することが求められる。

このように、伝統的金融と分散型金融では、サービス提供者や取引主体、監督のあり方（信用の根拠）に違いがあるほか、適用されている技術やエコシステムに所属するプレイヤーも異なるが、IOSCOのレポートに、「暗号資産市場と伝統的な金融市場間の公平な競争環境を促進し、規制の裁定リスクを低減するため、DeFi（既存または新規）に対する規制の枠組みは、伝統的な金融市場で要求されるものと同じ、または一貫性のある、投資家保護と市場のインテグリティに対する規制の成果を達成することを目指すべきである。」とあるとおり、分散型金融に対して、伝統的金融で培われた規制の枠組みをもとに監督のあり方を見直す必要性があると議論されるようになっている。

- Chainalysisによると、ここ数年、暗号資産の盗難規模が拡大傾向にあり、2022 年は37 億ドルが盗難被害にあった。2023 年には、前年比約 54.3% 減少して 17 億ドルとなったものの、ハッキング事件の数は 2022 年の 219 件から 2023 年の 231 件へと増加している。

図表1-3-1　暗号資産の盗難推移



- これらのリスクの顕在化を受けて、当局による暗号資産及びDeFiに対するリスク認識は高まっている。
- FATFにおいては、DeFiと称するアレンジメントであっても、一定の者がコントロールもしくは十分な影響力を持っている場合には、（中央集権型の暗号資産取引所等と同様に）FATF基準の対象となることが指定されている。一方で、規制主体の特定や執行可能性の担保における課題も指摘。
- EUの暗号資産市場（MiCA）規制では、完全に分散化されたサービスが対象外となっており、分散型金融の仲介者に規制を拡大するためには、「暗号資産サービスプロバイダー」の定義を見直す必要がある、としている。
- DeFiに対して様々な規制アプローチが模索されており、例えばフランス中銀が公表した研究ペーパーにおいては、認証による規制がブロックチェーンインフラのセキュリティを強化し、DAOが法人格を持つことで監督され、分散型金融サービスへのアクセスを提供する仲介者に対するコントロールによって顧客保護を強化できると提案されている。
- このような要請も踏まえ、分散型金融システムのなかには、自主的に監督対応機能の実装を目指す動きがある。

出典：Chainalysis「Stolen Crypto Falls in 2023, but Hacking Remains a Threat」https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/
FATF https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

ここでは、分散型金融システムに関連して、事業者やソリューション提供者による、ML/TF等のリスク低減に向けた取組事例を紹介する。

Fireblocksによるトークン送金前の脅威度確認機能

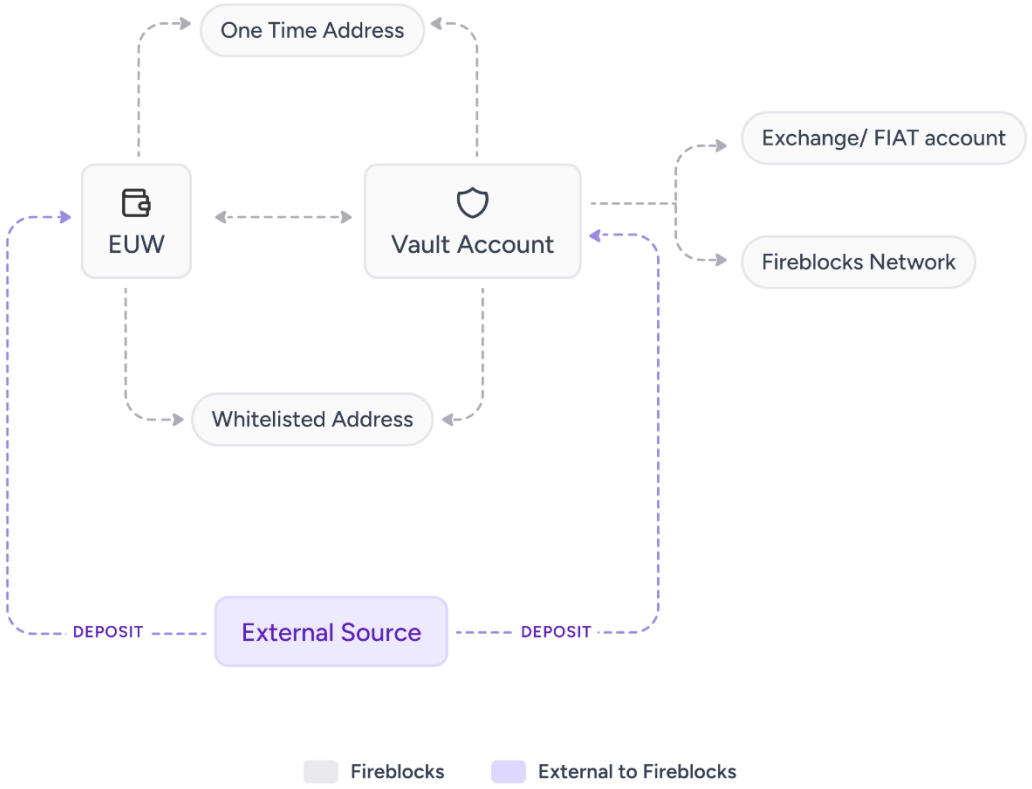
米・Fireblocks社はデジタル資産の保管、取引、発行、管理などを包括的に支援するプラットフォームを提供している。

同社のプラットフォームでは、疑わしいスマートコントラクト、フィッシングサイト、危険なdApp(decentralized application)とのやり取りを防ぐことを目的とするリアルタイムの脅威検知アラート機能及びスマートコントラクトとのやり取り時にトークン残高の推定変化をプレビューできる機能を提供している。

トークンの送金先、送金元、送金システムを決済完了前に把握したうえで、脅威度判定を利用者に助言するといった仕組みは、分散型金融システムでは取引相手が誰だかわからないことが多いことから、当該ニーズが存在すると考えられる。

図1-4-1は、Fireblocks 社が想定している取引の流れの例として、利用者の金庫型アカウント (Vault Account) あるいは埋め込み型のユーザーウォレット (EUW) からの出金に際し、出金先のアドレスの妥当性をホワイトリストアドレスを参照して判断してから外部アカウント (Exchange/FIAT account) に送金する流れを示している。

図1-4-1　Fireblocks社が想定している取引の流れ



出典：Fireblocks Fireblocks expands DeFi security capabilities to protect institutions from ever-evolving threats
https://www.fireblocks.com/blog/fireblocks-expands-defi-security-capabilities-to-protect-institutions-from-ever-evolving-threats/
https://ncw-developers.fireblocks.com/docs/transaction-flows

Uniswapによる金融取引の制限機能

Uniswapは、DEXとして、スマートコントラクトに暗号資産の取引を行うプラットフォームを提供している。

ブロックチェーン分析企業のTRM Labsとの提携後、横領や制裁に関連するウォレットアドレスに対し、アクセス制限を進めていると公表している（TRM Labが、制裁、テロ資金調達、ハッキングや盗難資金、ランサムウェアなどに関与するウォレットアドレスを特定し、Uniswap側が当該アドレスをブロック）。ブロック対象を示すuniswap-trm.csvがGITHUBに公表されており、「詐欺、ハッキングもしくは盗難されたファンド、制裁」などにカテゴライズされたウォレットアドレスが596個、掲載(2024/5/21現在)。

特定のウォレットアドレスに対してアクセス制限を行い送金を制限する仕組みは、銀行口座を凍結して送金を制限する仕組みと類似しているとも評価できる。

図1-4-2　UNISWAPのソースコード（抜粋）

```
6  export default function useAccountRiskCheck(account: string | null | undefined) {
7    const dispatch = useAppDispatch()
8    const { isBlocked, isBlockedLoading } = useIsBlocked(account || undefined)
9
10   useEffect(() => {
11     if (!account) {
12       return
13     }
14
15     if (isBlockedLoading) {
16       return
17     }
18
19     if (isBlocked) {
20       dispatch(setOpenModal({ name: ApplicationModal.BLOCKED_ACCOUNT }))
21     }
22   }, [account, isBlockedLoading, isBlocked, dispatch])
23 }
```

図1-4-2 は、Uniswap のウェブアプリケーションにて、上記のブロック対象であるかどうかを確認し、対象であればその旨のダイアログウィンドウを表示する処理を示している。Uniswap はあくまで分散型金融であることを標榜しているので、プロトコルではブロック処理を行わず、自社が提供するウェブアプリケーション上の処理としてこれを行っている。

出典：Uniswap Labs Address Screening Update https://blog.uniswap.org/trm

GITHUB uniswap-trm.csv https://gist.github.com/banteg/1657d4778eb86c460e03bc58b99970c0

GITHUB useAccountRiskCheck.ts https://github.com/Uniswap/interface/blob/96851c80644aa24413d65dca54efdb344d0d7955/apps/web/src/hooks/useAccountRiskCheck.ts

Circleによる金融取引の制限機能

Tornado Cashという暗号資産の取引の詳細を不明瞭にできるミキシングサービスが、北朝鮮のハッキングシンジケートであると目される「Lazarus Group」を含め、複数の暗号資産のハッキングによる収益の洗浄に利用された疑いで、米国財務省がTornado Cashに関連するイーサリアムおよびUSDCウォレットアドレスをいわゆるブラックリストに計上した。

この米国財務省からの制裁措置に対応し、Circle社は、該当するUSDCウォレットアドレスに保持されているUSDCを凍結対象とした。イーサリアムのブロックチェーンエクスプローラー（Etherscan）のデータによると、少なくとも75,000USDCが凍結対象とのことだった。

図1-4-3はブラックリストに該当するアドレスであるかどうかの判定処理や、ブラックリストにアドレスを追加・削除する処理を示すソースコードを公表資料から抜粋したもの。

図1-4-3　Circle社のソースコード（抜粋）

```
59          * @notice Checks if account is blacklisted.
60          * @param _account The address to check.
61          * @return True if the account is blacklisted, false if the account is not blacklisted.
62          */
63         function isBlacklisted(address _account) external view returns (bool) {
64             return _isBlacklisted(_account);
65         }
66
67         /**
68          * @notice Adds account to blacklist.
69          * @param _account The address to blacklist.
70          */
71         function blacklist(address _account) external onlyBlacklister {
72             _blacklist(_account);
73             emit Blacklisted(_account);
74         }
75
76         /**
77          * @notice Removes account from blacklist.
78          * @param _account The address to remove from the blacklist.
79          */
80         function unBlacklist(address _account) external onlyBlacklister {
81             _unBlacklist(_account);
82             emit UnBlacklisted(_account);
83         }
```

出典：https://x.com/jerallaire/status/1557004767930499072

https://github.com/circlefin/stablecoin-evm/blob/master/contracts/v1/Blacklistable.sol

Circle Pledges Action on User Privacy After Freezing $75K Tornado Cash-Linked USDC https://beincrypto.com/circle-pledges-action-after-freezing-75k-tornado-cash-linked-usdc/

VC/DIDを活用したAML/CFTとプライバシーの両立に向けた取組

暗号資産取引所を運営するコインベース（Coinbase）やUSDCを発行・運営するサークル（Circle）などが、検証可能な資格証明書である Verifiable Credentials や分散型ID である DID といった標準仕様に基づく、Verite と呼ばれるプロトコルを公開している。

当プロトコル は、利用者が個人データを開示することなく、資格情報を発行できる。当プロトコルの利用が想定されるユースケースとしては、認定投資家のステータス、社会的評判、NFT出所追跡などとされている。これらの資格情報はデジタル資産と同様にウォレットに保存できる。資格情報は利用者が所有するため、さまざまな組織やプロトコルが ID 証明書にいつどのようにアクセスするかを制御できる。

Veriteは分散型金融システムのRegTechにどう役立つか

Veriteが使用されている分散型金融システムでマネー・ローンダリングが発生した場合、分散型金融システム運営者や当局等が犯罪者を特定できるかどうかは、いくつかの要因に依存する。以下のようにKYC情報の事前収集や取引の透明性が確保されている場合にマネー・ローンダリングが発生した場合であれば、適切な手続きと技術を用いることで、当局は犯罪者を特定できる可能性がある。

１）資格証明書に関わる個人情報の開示が可能であること

資格証明書自体には個人を特定できる情報は記載されていなくても、正当な手続きにより証明書の発行者に開示を要求すれば必要な情報が得られるように設計・運用されていること。

２）KYC（Know Your Customer）情報の正しさ

分散型金融システムの利用登録時に、ユーザーのKYC情報を収集し、しかるべき主体がKYC情報の真贋を確認し、KYC情報を然るべき手続きを経れば取得可能なようにオフチェーンで記録していること。

３）プライバシーと匿名性のバランス

DID に対する資格証明が KYC を経ないのであれば匿名性を固持することも可能であるため、犯罪者が匿名性を悪用するリスクもありうる。当局等が適切な法的手続きを経て情報開示を求める仕組みをあらかじめ保つこと。

出典：Verite Verite Verification Service https://developers.circle.com/verite/docs/verite-service

図1-4-4 は Verite による典型的な処理フローを示したもので、ユーザーを示すウォレット側が、発行フローで検証可能な資格情報(VC)を取得し、DeFi アプリケーションである Dapp側は、トランザクションを実行する前に検証フローで VC を検証している旨を示している。具体的には以下の通りである。

(1) ウォレット保有者から証明書のイシュアーに対して
　資格証明書の申請を送る。

(2) KYC (Know Your Customer) または KYB (Know Your Business) の後に、
　イシュアーが資格証明書 (VC) を発行する。
　VC はウォレットに保管される。

(3) ウォレット保有者は DeFi アプリケーションの利用を希望する。

(4) アプリケーションは VC をリクエストする。

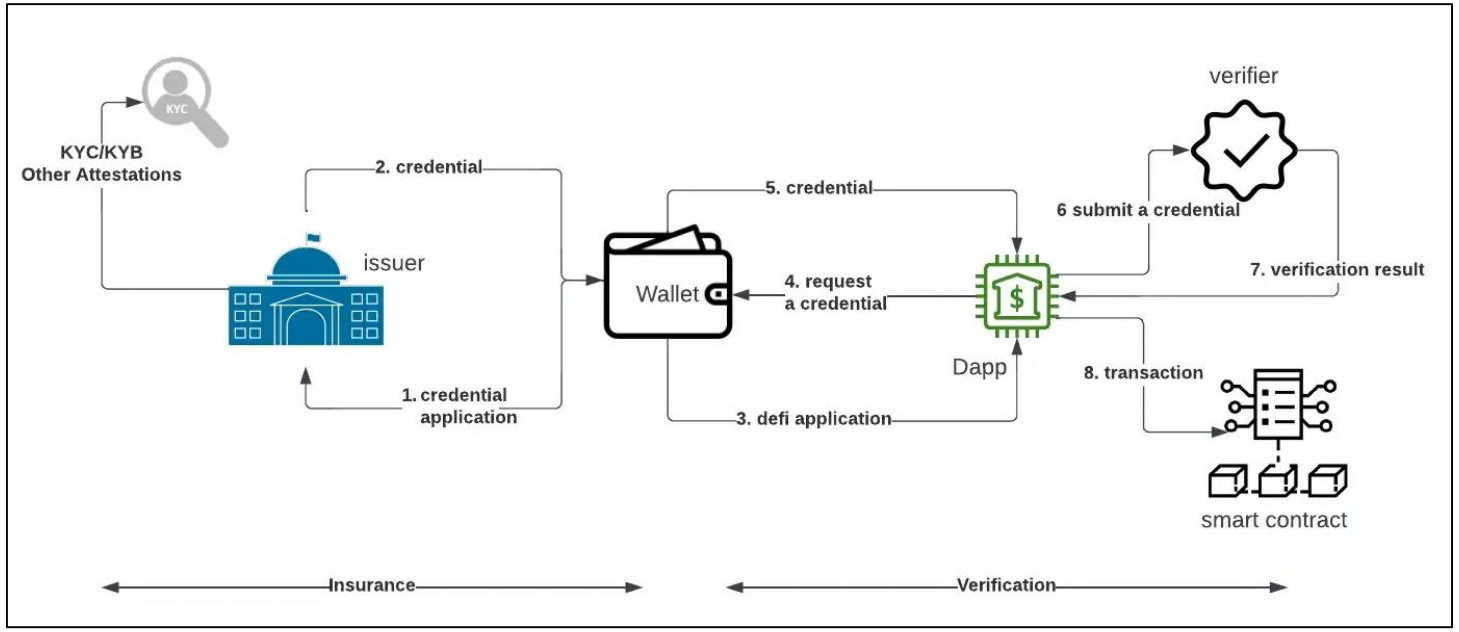
(5) ウォレットは VC を提示する。

(6) アプリケーションは検証者に VC を提出する。

(7) 検証者は検証結果をアプリケーションに送る。

(8) アプリケーションはトランザクションを発行する。

図1-4-4　Verite の処理フローイメージ



出典：Verite Verite Verification Service https://developers.circle.com/verite/docs/verite-service

Project GuardianによるRegulated DeFiの検証

伝統的金融側によるDeFiレンディングプロトコルAAVEを活用したプログラム化（トークン化）の検証事例として、以下にProject Guardianによる取り組みを紹介する。

MASが2022年5月に設立したデジタル資産に関する官民連携イニシアチブ「Project Guardian」の目的は、金融安定や公正性に係るリスクを管理しつつ、アセット・トークナイゼーション等のデジタル技術の活用可能性について、パイロット実験を通じて検証を行うことにある。債券・外国為替取引・資産運用等の分野でパイロット実験が行われており、デジタル資産領域への知見を深め様々なアセットクラスのユースケースを調査するため、金融機関や政策当局の参加を促す。

なお、本プロジェクトには、 JPモルガン、DBS銀行、SBIデジタルアセットホールディングスなどの民間企業が参加しているほか、金融庁がオブザーバーとして参加している。

以下に、「デポジット預金トークンの発行と交換、トークン化された国債の売買」に関するパイロット実験について示す。

・取引基盤にはDeFiレンディングプロトコルのAAVEの修正版などが使用されている。

・検証内容はホールセールにおけるトークン化アセットのクロスカレンシー取引が直接参加者間で即座に取引・清算・決済できるかどうか、トークン化された負債の規制上の扱いや、トークン化された資産取引の規制とリスク管理への影響など

このほかにも、「ウェルスマネジメント」、「貿易金融」についてもパイロット実験を行っている。

出典：MAS First Industry Pilot for Digital Asset and Decentralised Finance Goes Live
https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live
MAS Proposes Framework for Digital Asset Networks　https://www.mas.gov.sg/news/media-releases/2023/mas-proposes-framework-for-digital-asset-networks

図1-4-5 Project Guardianによる検証構成例

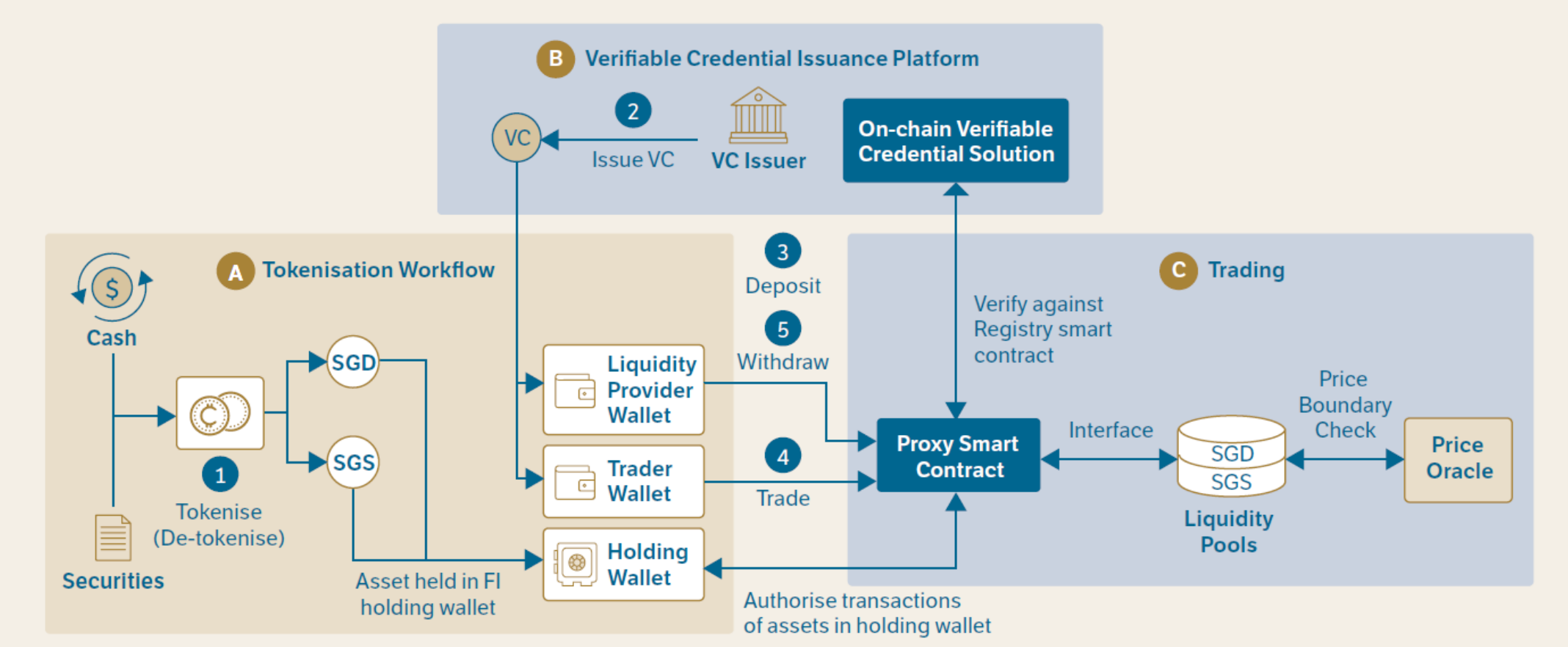


図1-4-5はProject Guardianによる取り組みのひとつとして、DBS銀行とSBIデジタルアセットホールディングスが協力して、トークン化されたシンガポール国債（SGS）債券、日本国債（JGB）、日本円（JPY）、シンガポールドル（SGD）で構成される流動性プールに対して外国為替および国債取引を実行する可能性を検証した際のシステム構成を示している。さまざまなシステムで検証しているが、そのうちのひとつにAAVEがある。

出典：https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/project-guardian/project-guardian-open-interoperable-network.pdf

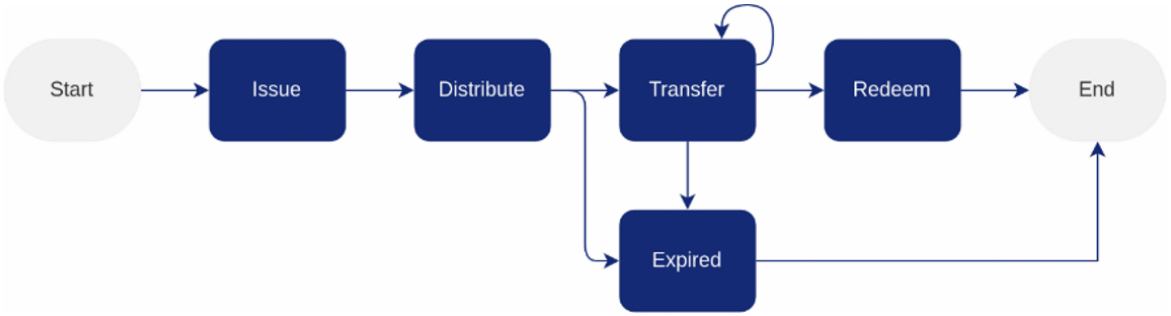
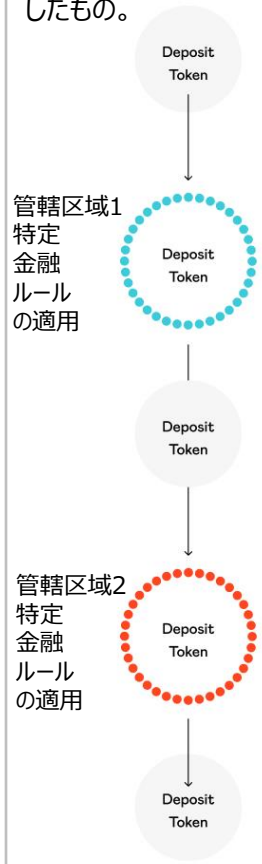
５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

- ここからは、当局・中央銀行や銀行等の伝統的金融機関が関与するトークナイゼーションのプロジェクト（非暗号資産）について、公表文献等から概要を整理して共通点の把握を行う。

- 本章において調査対象としたプロジェクトは以下の７件とした。
  - Purpose Bound Money（シンガポール金融管理局　以下、MAS）
  - Project Guardian（MAS）
  - DREXプロジェクト（ブラジル中央銀行　以下、BCB）
  - Project Mariana（国際決済銀行　以下、BIS）
  - JPM Coin（Onyx / JP Morgan）
  - Project Ion（DTCC）

- 調査対象プロジェクトから、公表文献をピックアップして次の観点で整理した。
  - プロジェクトの目的
  - 金融安定や利用者保護等に関連する研究内容、研究結果
  - 便益とリスク

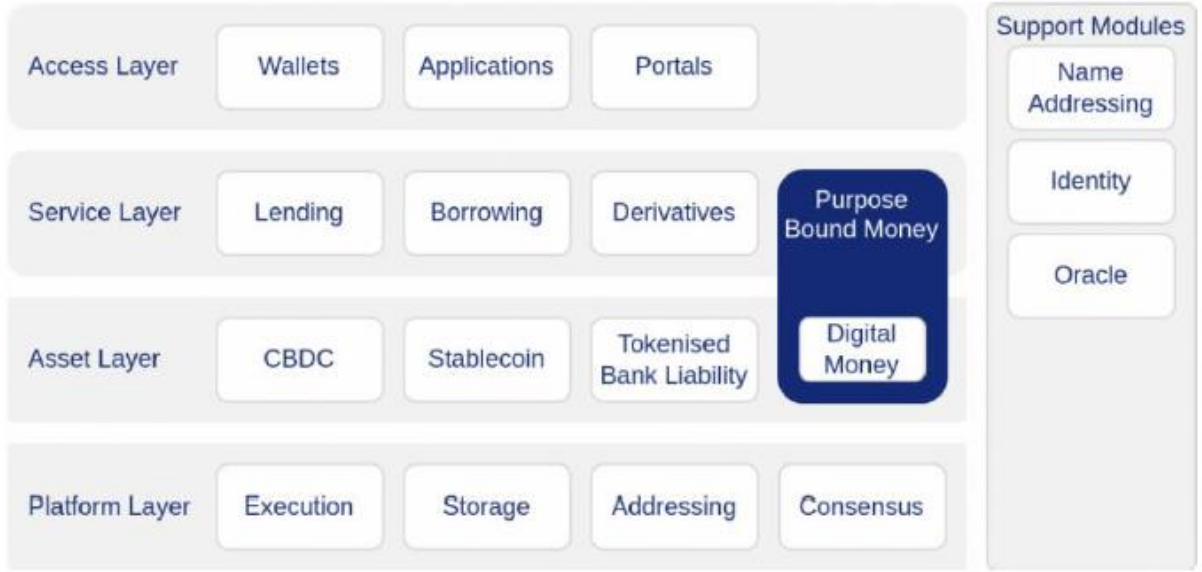
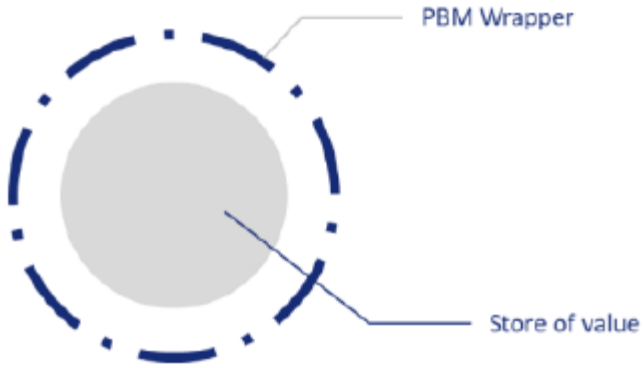
５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

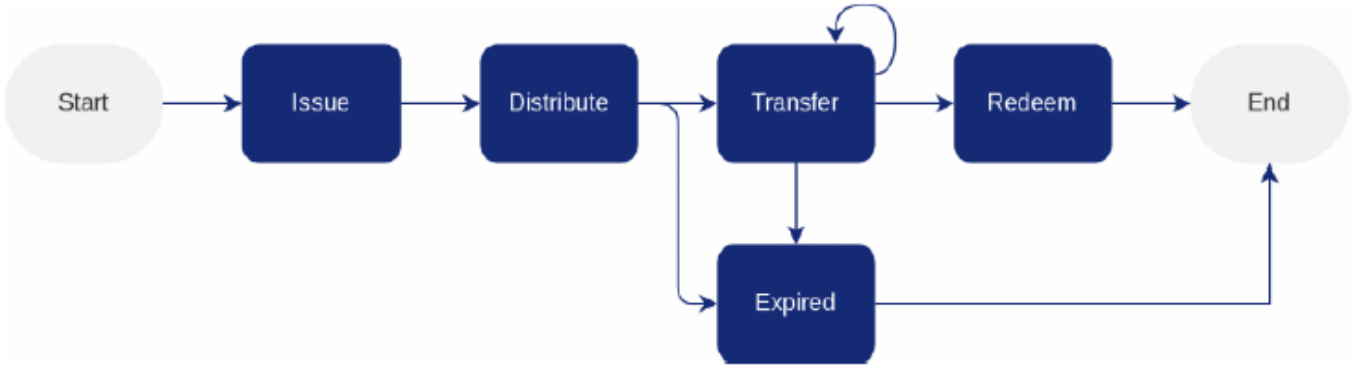
プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
Purpose Bound Money （Project Orchid）	本文献の対象は特定のブロックチェーンに限られていない （Ethereumチェーンのトークン規格であるERC721・ERC1155を実装することが可能である旨の記載はある）	Purpose Bound Money (PBM) Technical Whitepaper	MAS	2023年6月	【概要】 本文献は、通貨に用途を組み込み、使用目的を制限するデジタルマネーのことを「Purpose Bound Money」(以下PBM)と呼称し、その技術的な概要を解説したものである。なお、類似の概念にProgrammable Moneyがある。MASは、Project Orchidと呼ばれるプロジェクトを主導しており、PBMのガイダンス策定、実証実験に取り組んでいる。本調査対象はProject Orchidのフェーズ1。 以下の図は、PBMトークンのライフサイクルを示している。  【プロジェクト参加者】 IMF、イタリア中銀、韓国銀行、フィンテック企業など 【研究内容】 個々の無記名資産に固有の特性をプログラミングし、デジタルマネーの用途を制限することが可能である。一方で、デジタルマネーに直接プログラミング・ロジックを実装することで、自由な交換可能性が制限される側面も持っている。 デジタルマネーに直接プログラミングロジックを実装した場合は、新しい使用条件や使用例が必要になるたびに、流通しているすべてのデジタルマネーをプログラムし直す必要がある、また、デジタルマネーの発行者が、それぞれ異なるプログラミングロジックが実装された複数のバージョンのデジタルマネーを提供することも考えられるが、これらのデジタルマネーは互換性がなく、市場の流動性を阻害する可能性がある。 本文献では、デジタルマネーを自由に交換できるようにし、デジタルマネーの互換性を維持するために、さまざまなモデルを研究している。	以下の図は管轄区域間を移動し、管轄区域固有のルールが適用されるデポジット トークンを示したもの。 

出典：A Singapore Government Agency Website https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/purpose-bound-money-whitepaper

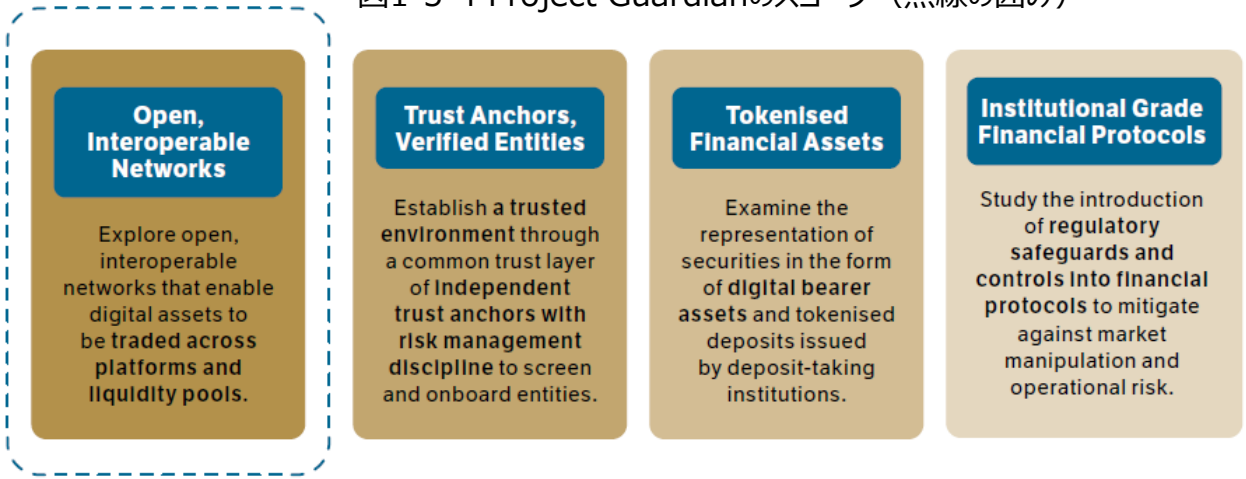
５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
Purpose Bound Money （Project Orchid）	【目的】 本プロジェクトは金融セクターにおけるデジタル化の取り組みに対する課題として、決済スキームとプラットフォームの急増を背景として、相互運用可能な決済システムの必要性を認識し、貨幣のプログラム化と換金性およびプログラム化のモデル検討を目的としている。 【便益】 PBMの機能は、プリペイドパッケージ、オンラインコマース、契約締結、商業リース、貿易金融、寄付金、クロスボーダー決済の利便性を向上させる可能性がある。 • 「プリペイドパッケージ」として、企業が商品を製造したりサービスを提供したりする前に、保証として前もって料金を徴収する必要がある場合に利用できる。消費者が事前に約束した金額を「引き出す」前に、企業が義務を果たすことを保証する支払い条件を含めることで、不渡りのリスクを解決することができる。 • 「クロスボーダー決済」として、AML/CFT等の既存の規制要件を条件としてPBMに組み込むことで、コンプライアンスチェックを自動化することができ、クロスボーダー決済におけるコストを大幅に削減し、効率を高めることができる。国境を越えた決済を強化するためのG20ロードマップに照らし合わせると、規制と政策の相互運用性に貢献する可能性がある。 • 「寄付金」として、高い透明性と説明責任を果たす。例えば、PBMを利用することで、意図した受益者のみが、特定の条件が満たされた場合にのみ、資金を使用できるようにすることができる。 • 「貿易金融」として、企業が国際貿易取引のリスクや複雑さを管理するのに役立つ。国境や通貨が異なる複数の当事者が関与する貿易を円滑化するため、貿易金融業者は信用状、銀行保証、書類による回収などのサービスに対し、支払いが安全かつ効率的に行われるよう支援すると同時に、不払いや詐欺のリスクからも保護する。 • 「商業リース」として、賃貸借契約の当事者が敷金を全額回収できる可能性を保証されている場合、敷金の役割を果たすことができる。紛争が発生した場合は、紛争が解決するまでPBMを一時停止することができる。 【リスク】 • 現在、ほとんどの小売ユーザーはデジタル資産ウォレットの使用に慣れておらず、この不慣れさが悪意のある者による悪用のリスクを高めている。これを軽減するために、スマートコントラクトウォレットとしても知られるアカウント抽象化を利用することで、デジタル資産取引のユーザーエクスペリエンスとセキュリティを向上させることができる。この技術により、ユーザーが基礎となる技術を理解することなく、アカウントの回復、取引制限、紛失したアカウントの凍結などの機能を実現することができる。 • 価値貯蔵ではなく、支払い義務を表す、目的拘束型トークンの形態では、決済がアトミックかつリアルタイムではなく、遅延ベースで行われるため、決済失敗のリスクにさらされる。 • 遅延送金やサプライチェーンの支払い管理など、複雑なロジックをコンポーネントに統合しようとする場合に懸念される悪意のあるコードの導入。対策として、独立した監査や信頼できる外部の第三者機関をオラクルとして入力元とする点をあげている。

プロジェクト名	プロジェクト概要
Purpose Bound Money （Project Orchid）	【PBMの技術的な概要】 • システムの構造 PBMはさまざまなタイプの台帳や資産で機能することを目指している。PBMは分散型台帳と非分散型台帳の両方に実装できることが想定されている。PBMのプロトコルは、4つのデジタル資産に関わるレイヤーモデル（アクセスレイヤー、サービスレイヤー、アセットレイヤー、プラットフォームレイヤー）のうち、プログラミング・ロジックはサービスレイヤー、デジタルマネーはアセットレイヤーとなる。デジタルマネーをPBMとして束ねる場合、サービスレイヤーとアセットレイヤーをまたぐ（図1-5-1参照）。 図1-5-1 PBMにおけるシステムアーキテクチャの概要  図1-5-2 PBMの構成要素  • 構成要素 PBMは、使用目的を定義するPBMラッパーと、担保となる基礎的な価値貯蔵機能から構成される（図1-5-2参照）。PBMラッパーは、PBMが、特定の期間内、特定の小売店、所定の額面での有効性など、意図された目的でのみ利用できるようにプログラムすることができる。PBMラッパーで指定された条件が満たされると、デジタルマネーは解放され、受取人に送金される。PBMによって制限されたデジタルマネーは、PBMの担保として機能する。PBMの条件が満たされると、デジタルマネーは解放され、所有権は対象となる受取人に移転する。デジタルマネーは、貨幣の機能を満たさなければならない。

プロジェクト名	プロジェクト概要
Purpose Bound Money （Project Orchid）	• 役割と相互作用 PBMにおけるエコシステムでは、エンティティが複数の役割を保持することも、1つの役割を異なるエンティティが実行することも可能である。 PBMクリエイター：PBM内のロジックの定義、PBMトークンの鋳造、配布を担当する。 PBMホルダー：1つ以上の PBM トークンを保有する。このエンティティは期限切れでない PBM トークンを交換できる。 PBMリディーマー:PBMトークンが送金される際に、その原資となるデジタルマネーを受け取る。 • ライフサイクル ライフサイクルは、交付、分配、譲渡、償還、失効の段階に示すことができる（図1-5-3参照）。交付では、PBMスマートコントラクトが作成され、PBMトークンが鋳造される。分配では、PBMトークンは、鋳造された後、PBMクリエイターによって、PBMホルダーに配布され、使用される。譲渡では、PBM トークンはラップされた状態で、そのプログラムされた規則に従って、あるエンティティから別のエンティティに転送される。償還は、PBMで指定された条件がすべて満たされた後に実行され、PBMトークンはラップを解かれ、トークンの所有権は、受領側のエンティティに移転される。失効は、PBMで指定された条件のいずれかが明白に違反または期限切れとなり、PBMトークンがPBM保有者にとって永久に使用できなくなった状態を指す。 図1-5-3 PBMのライフサイクル  • シーケンスの流れ 本文献では、PBM を 3 つのコンポーネントに分割した設計を検討している。(1)ホワイトリストとブラックリストによるアクセス制御、(2)PBMラッパーの有効期限、(3)PBMトークン・タイプの有効期限 • 設計上の考慮事項 本文献では、相互運用性、デジタルマネー、プライバシー、政策に関する考察、デジタルレディネス、セキュア・プログラミングの観点から検討がなされている。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
Project Guardian	許可型ブロックチェーン	オープンで相互運用可能なネットワークの実現	BISの決済および市場インフラストラクチャ委員会	2023年6月	【概要】 本文献は、プロジェクト ガーディアンの基本原則の1つであるオープンで相互運用可能なネットワークの構築に焦点を当てている。ネットワークや流動性プールをまたいでデジタル資産の取引を可能にする設計オプションを理解するためのフレームワークが紹介されている。このフレームワークでは、金融市場インフラストラクチャの中核原則を考慮し、これらのトピックの限界を押し広げようとしたプロジェクトを参考にしている。本文献は、参加金融機関の協力を得て、BISの決済および市場インフラストラクチャ委員会の専門家と共同で作成された。 【プロジェクト参加者】 DBS Bank、HSBC、SBI Digital Asset Holdings、United Overseas Bank、Marketnode、Standard Chartered、ONYX by J.P.Morgan 【研究内容】 本文献では、トークン化された実物経済資産と金融資産をベースに、オープンで相互運用可能なデジタル資産ネットワークを設計するためのフレームワークを紹介する。 図1-5-4 Project Guardianのスコープ（点線の囲み）  Figure 1: Guardian Themes	金融庁とMASは、2017年３月に両当局が締結したフィンテックに係る協力枠組みに基づき、MASが2022年5月に設立したデジタル資産に関する官民連携イニシアチブ「Project Guardian」に金融庁がオブザーバーとして参加することを発表している（2024年６月26日）。

出典：https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks

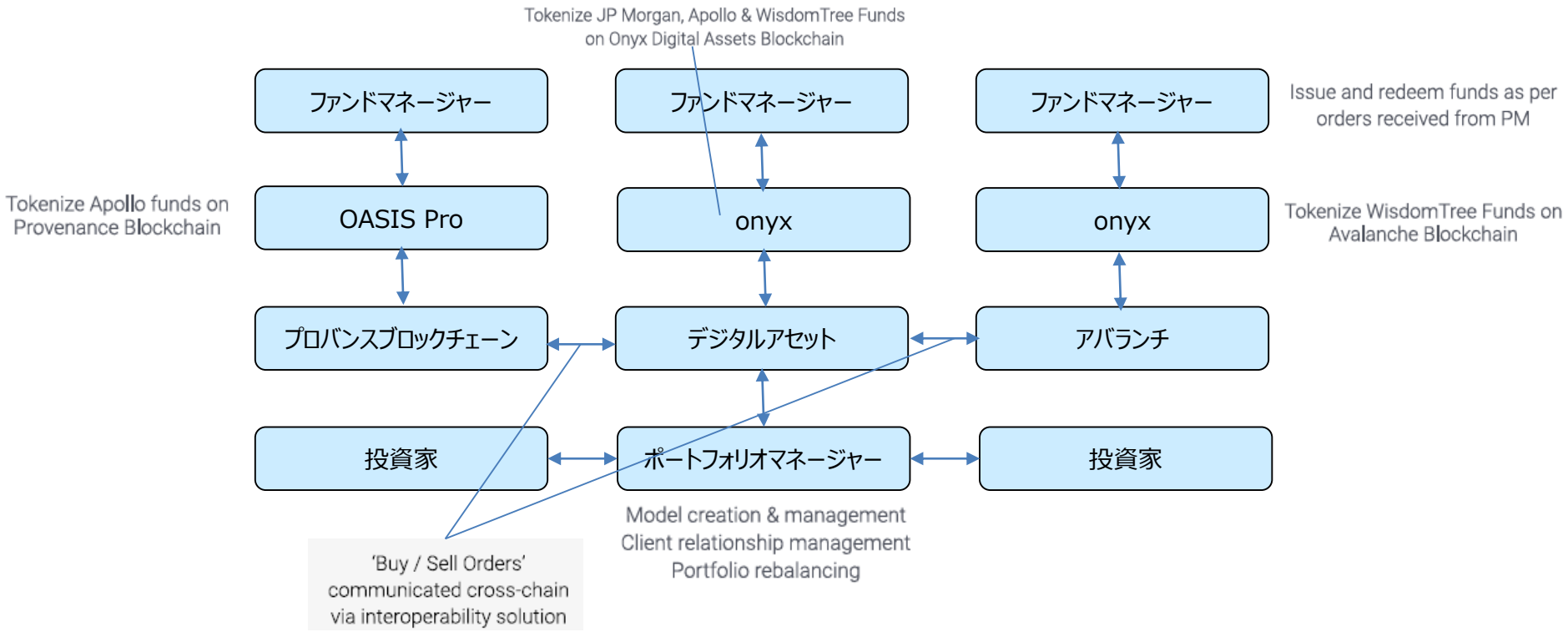
５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
Project Guardian	【目的】 プロジェクト・ガーディアンは、業界におけるベストプラクティスと技術標準を向上させることを目的としている。デジタル資産や分散型プロトコルの普及に伴う市場の断片化を防ぐ。このプロジェクトはまた、参加者が認証された当事者とのみ取引できるように、認証情報を審査、検証、発行するトラスト・アンカーとしての規制金融機関の役割を模索する。 【便益】 • 信頼できる第三者や中央機関を介さずに、異なるブロックチェーン間での直接的な資産交換を可能にする技術のひとつとして、HTLC（Hashed TimeLock Contract）を紹介する。HTLCは、異なるネットワーク上のスマート・コントラクトを通じて実装されたハッシュ・ロックとタイム・ロックのセットを使用する。アトミックスワップや、支払いチャネルネットワークで活用される可能性がある。 • 「ホワイトリストのサービスプロバイダー」はそのサービス・機能へのアクセス可否を判断するため、参加者を個別に自動的に審査できる。他方、サービスプロバイダーには、適切なリスク・コンプライアンス・プロセスと管理体制を確保する必要がある。 • 貿易条件貿易・決済プロセスにおいて、取引執行における業務効率化と決済リスクの軽減に貢献する。 • デジタル資産ネットワークの斬新の特徴として、即時決済を含む決済サイクルの短縮が考えられる。他方、これは信用リスクと流動性リスクの双方に影響を与える。決済を迅速化（または即時化）すれば、代替コストリスク（信用リスクの一種）を低減（または排除）できるため、必要な証拠金の額を削減（または排除）できる可能性がある。しかし、この場合、取引前に現金やデジタル資産を事前に準備する必要があり、流動性コストが増加する可能性が高い。 • デジタル資産ネットワークにはトークンの発行、上場、登録、取引／市場形成、資産サービシング、信用供与などの機能を提供する。他方、これらの機能に対し、信用リスクや流動性リスクをもたらす可能性がある。 【リスク】 • 「バリデーター」がプラットフォームの運営組織によって許可された既知の存在であり、記録されるトランザクションの整合性を保証する役割を果たす。バリデーターはそのサービスの提供により、報酬を受け取る。バリデーターは規制された金融機関が担うことがあり、技術的なリスク管理の対象となる。 • デジタル資産ネットワークは分散型であるため、複数の司法管轄権を有する環境で運営される可能性が高く、潜在的な抵触から生じるリスクがある。 • 継続企業として存続できない懸念が、広範な金融市場にシステミック・リスクの影響を及ぼす可能性がある。なかでも、デジタル資産ネットワークを支える運用体制（DLT等）がオペレーショナル・リスク原則の遵守にどのような影響を及ぼすかについて検討が必要である。 • パーミッションレス・ネットワークは、攻撃の複雑さと潜在的な脆弱性を増大させる。そのため、ソフトウェアやスマート・コントラクトが攻撃を受けるリスクがある。 • 規制対象の金融機関によって管理されていないオープンソースのパブリックプロトコルを使用することは、基盤となるソフトウェアがフォークされたり拡張されたりする可能性がある。 • 取引されるトークンとその裏付けとなる資産との間の流動性と成熟度のミスマッチの可能性がある。例えば、トークン化された資産は、そのトークンの裏付けとなる資産を提供する可能性があるが、トークン化された資産が、満期プロフィールが一致しない準備資産に裏打ちされている場合、償還実行リスクシナリオが増加する可能性がある。 • 公開された無許可のプラットフォームの流通力が活用されており、アクセスが容易である反面、金融の安定性と完全性にリスクをもたらす可能性がある。Guardianでは、当リスクに向けフレームワークを提案する。 • デジタル資産の保全に対する責任が、匿名の法人を含む複数の事業体に分散している場合、実証することが困難となるリスクがある。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
Project Guardian（Wealth Management）	許可型ブロックチェーン	ウェルス・マネジメントの未来 トークン化を活用した伝統的投資とオルタナティブ投資の超効率ポートフォリオ	JPモルガン、アポロ	2023年	【概要】 MASはProject Guardianの取り組みにおいて、海外の金融当局や海外企業と共同研究や実証実験を実施している。本文献はMASの共同イニシアチブであるProject Guardianの下で実施された実証実験について、許可されたブロックチェーンネットワーク上で資産のトークン化とクロスチェーンの相互運用性を模索し、J.P.モルガンとアポロが協働で研究結果を報告したもの。 【プロジェクト参加者】 JPモルガン、アポロなど 【研究内容】 本文献では、ウェルス・マネジメント業界における現状について、裁量的ポートフォリオ管理（投資家自身の投資方針や金融目標、リスク許容度を定め、日々の投資決定をポートフォリオマネージャー（以下、PM）に委託する投資管理手法）には限界があるとしている。 そこで、トークン化によってポートフォリオ管理における公的資産と私的資産の扱いを調和させ、アセットマネージャー、ウェルスマネージャー、投資家に大きな価値を生み出す方法を提案し、シームレスなポートフォリオ管理のためのスケーラブルな次世代システムの提供について概念実証を行う。概念実証では、利点と考慮事項を分析する。 【目的】 MASが推進する、ホールセールの資金調達市場の効率化と流動性向上を目的としたプロジェクト。トークン化やDLTを活用した新たな金融市場インフラの構築を目指す。	－

出典：https://www.jpmorgan.com/onyx/documents/portfolio-management-powered-by-tokenization.pdf

プロジェクト名	プロジェクト概要
Project Guardian（Wealth Management）	具体的な検証は以下のとおり。PMがあるモデルの目標資産配分を更新することで、そのモデルを追跡するすべての投資家のポートフォリオのリバランスをシステムが自動的に行う。さらに、投資家がより多くの投資資金を投入する際、モデルに含まれる資産の種類や、それらの資産がどのチェーンに記録されているかにかかわらず、システムがモデルに従って自動的に適切な配分の注文を発注し、決済する。ファンドをトークン化し、裁量的ポートフォリオをスマートコントラクトとして表現することで、何万ものポートフォリオを代表的なモデルにプログラムでリンクさせ、そのモデルに変更が生じたときに自動的に一括してリバランスする。これらのPOCエコシステムとポートフォリオ管理ソリューションのイメージを以下に示す。 図1-5-5 エンドツーエンドのポートフォリオ管理と相互運用性の概念実証  図1-5-4は本文献から図を抜粋し、当社が簡略加工したもの

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
Project Guardian（Wealth Management）	【便益】 • 効率性の向上：スマートコントラクトを活用して資産の所有権を表し、記録することで、PMと運用の役割を単一の自動化されたプロセスに統合することができ、ポートフォリオを大規模にプログラム的に展開し、リバランスすることが可能になる。共有台帳上に現金とファンドの所有権記録が存在し、スマートコントラクトが有効な取引執行と組み合わされることで、コストのかかる照合の必要性や取引エラーの発生を抑制できる。規模が拡大すれば、時間とコストの節約により、ウェルス・マネージャーはリサーチや、アルトコインがどのようにポートフォリオに組み入れられるかについて顧客を教育するような、顧客向けのサービスに再投資できるようになる。効率化のメリットは、資産運用会社、ファンド管理者、その他のサービス・プロバイダーなど、エコシステム内の他の企業にももたらされる可能性がある。投資家の視点に立てば、こうした摩擦のポイントを解消することで、PMはより安定的にフル投資を行うことができ、ポートフォリオのキャッシュ・ドラッグ（売却済み債権と新規購入債権の権利発生ギャップ等から投資家がバッファーとして備える、運用されない資金）を減らすことができる。平均的なPMが約3%の現金を保有し、バランスの取れたポートフォリオが長期的に現金より約8%多く生み出すことができると仮定すると、クライアントにとっての最終的な結果はコストが約24bps削減されることになる。 • 流動性向上の可能性：同じ台帳システム上で複数の関係者が情報を共有しやすく、トークン化された資産の所有権を簡単に移転できることから、アルトコインのような資産をブロックチェーン上で表現することで、これらの資産の流動性市場がより向上する可能性がある。今日、流通市場でアルトコインを売却するには、二者間で交渉する手作業が一般的である。これは個人投資家にとって問題となる可能性があり、取引を完了するのに必要な時間と事務手続きを考えると、保有資産が買い手を引き付けるのに十分な大きさでない場合が多いためである。スマートコントラクトを利用してこうした業務プロセスを簡素化し、引き受けと償還の自動ネッティングなどの代替流動性手法と組み合わせることで、さらなる流動性レバー（流動性を高めるための手段や方法）を追加できる可能性がある。 • オルタナティブ投資による投資成果の向上：上記のようなプロセスの合理化と流動性の向上により、オルタナティ ブ投資をポートフォリオモデルに組み入れることが可能となり、 投資家の期待リターンの向上やボラティリティの低減が期待できる。また、ポートフォリオモデルの変更に基づいてポートフォリオのリバランスを自動的に行うことも可能となり、目標資産配分からの乖離を最小化し、その結果、ポートフォリオがより最適な状態に近づく可能性がある。 • ロボアドバイザリーの効率性とアクティブ運用のアルファの融合：自動化されたポートフォリオ構築と運用は、ロボアドバイザリーサービスに似た合理的な経験を提供することができるが、専属のPMがつき、3つのアルファの源泉を通じてより高い潜在的リターンを得ることができる。1）アルトコインの組み入れ、2）アクティブ戦略に関するマネジャーのデューデリジェンス（例えば、トップクラスの大型成長ファンドの特定）、3）CIOのマクロなインサイトに基づくトップダウンの資産クラス・アロケーションの設定。 • 柔軟性と幅広いアクセス：相互運用性ソリューションを活用し、異なるブロックチェーン・ネットワークを接続することで、異なるチェーンにまたがるトークン化された投資へのアクセスが可能になり、PMは、そうでなければアクセスできない可能性のあるこれらの投資機会を含む総合的なソリューションを構築することができる。 【リスク】 • 投資ユニバース：トークン化された投資の世界は、クリティカル・マス（臨界量）に達する必要がある。つまり、ウェルス・マネージャーが展開可能な運用資産の数、資産クラス別に利用可能なトークン化されたサービスの幅、運用モデルに関するまとまりなどである。この分野では多くの発表が続いているが、今日、トークン化された投資で強固なポートフォリオを構築することはできない。トークン化された現実世界の投資の在庫総額は約13億ドル（https://app.rwa.xyz/ as of October 6, 2023）で、ほぼすべてがトークン化された米国債とプライベート・ローンで構成されている。ファンドマネージャーと投資家の双方から、さらなるトークン化投資の需要があるが、トークン化された投資の立派な市場が出現するには時間がかかるだろう。 • 流動性：本POCでは、投資家が投資ビークルに参入したり、投資ビークルから撤退 したりするメカニズムとして、ファンド・マネジャーとの間で直接行われる申込 みと償還を使用した。これを現実のものとするためには、この作業を拡大し、セカンダリー市場での購入と売却を検討することで、ポジションへの参入と撤退のあらゆる選択肢を検討できるようにする必要がある。オルタナティブ投資ファンドは一般的に伝統的な投資よりも流動性が低いため、さらなる流動性への配慮が必要となる。トークン化によって流動性が向上する可能性がある一方より効率的なセカンダリー・トランザクション・プロセスは、このテクノロジー自体が流動性を生み出すわけではない。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
Project Guardian（Wealth Management）	【研究結果】 POCでは、主に以下の項目について検討した。 • 複数の資産クラスや所有者登録にまたがる注文の執行と決済の効率性とスケーラビリティを向上させる方法。 • 伝統的な公的資産に比べて運用が難しく、流動性も限られているオルタナティブ投資を、一任ポートフォリオに組み入れる方法。 • 異なる技術プロトコルで開発された複数の所有者登録がもたらす断片化と相互運用性の課題を克服する方法。 • ブロックチェーン技術特有の技術的な複雑さを抽象化することで、多人数・多資産の共有台帳の利用を簡素化する方法。 POCを実施した結果、オルタナティブ投資を含む一任ポートフォリオを富裕層に提供することで、主要な関係者に以下のメリットを得られる可能性があった。 • ウェルス・マネージャー：例えば10万人の顧客ポートフォリオを持つウェルス・マネジメント会社は、毎月のリバランス・プロセスを3,000以上の操作ステップから数クリックに減らす。 • 投資家：プログラマティック・リバランスとほぼ即時の決済により、キャッシュ・ドラッグを排除することで、コストを20%近く削減する。 • 資産運用会社、ウェルス・マネージャー、ディストリビューター：富裕層へのオルタナティブ投資の幅広い販売を通じて、年間4,000億ドルの新たな収益機会を獲得する。 • サービス・プロバイダー（ファンド管理者、名義書換代理人など）：自動化とデジタル化を活用することで、効率性の向上、コスト削減、透明性の強化、リスクの軽減につなげる。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
DREXプロジェクト	Polygonなど	Lift Papers Revista do Laboratório de Inovações Financeiras e Tecnológicas LIFT論文 金融技術イノベーション研究室 ジャーナル 第5号	ブラジル 中央銀行	2023年 4月	【概要】 DREXは、ブラジル中央銀行（以下、BCB）が2020年から開発している中央銀行デジタル通貨（CBDC）プロジェクトであり、ブラジルの法定通貨であるレアル（BRL）に裏付けられる。 イノベーションを促進し、オープンで協力的な方法でアイデアを製品化する環境として、BCBがFenasbacと提携して、2018年に創設した金融・技術イノベーション研究所（LIFT）では、過去に256の提案がなされ、91のプロジェクトが選定され、そのうち76のプロトタイプが最終決定されてきた。本文献では、国家金融システムにおける革新のための最新の提案を提示する8つのLIFTラボ・プロジェクトに投資された検証結果を紹介している。 【プロジェクト参加者】 BCB、Fenasbacのほか、本文献には10数以上のテーマがあり、各テーマごとに銀行、フィンテック企業、技術プロバイダーなどが参加している。 【研究内容】 マイクロクレジットやReal Digitalと他のネットワークとの相互運用性、またNFC、オフラインQRコード、クレジットといったデジタルBRL（Pixと名付けられている）を対象とした機能を対象としている。加えて、本文献では、リアルデジタルのユースケースに焦点を当てたLIFTラボの特別版であるLIFTチャレンジプロジェクトを特集している。金融、非金融、暗号資産の売買に焦点を当てた9つのプロトタイプや、分散型金融、モノのインターネット、国際送金、オフライン決済に焦点を当てたプロジェクトが掲載されている。	「キャッシュレス経済への移行」という主な動機の下、決済システムとしてのCBDCの役割を越えて、イノベーションが日常生活にどのような影響を与えるために利用できるのか、また中央銀行が民間セクターと連携してイノベーションを促進する上でどのような重要な役割を担っているのかを示そうとしている。 世界中の中央銀行に対して、Real Digitalのインフラと LIFTの使用事例から、プログラム可能なCBDCの可能性（当局が経済的ショックの伝播状況を決済ネットワークデータに含まれる情報から解析できるなど）について教訓を与えることを目標としている。

出典：https://revista.liftlab.com.br/

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
DREXプロジェクト	【目的】 BCBはDREXの導入を通じて金融市場の効率化と金融包摂の促進を目指しており、そのリテール版DREXは規制対象の金融仲介業者によって提供される。金融仲介機関は要求払い預金や電子マネーの残高をDREXに変換し、その顧客が様々なインテリジェント金融サービスを利用できるようにする。リテール版DREXによって、国民はデジタル資産やスマートコントラクトを使った様々な金融取引にアクセスできるようになり、DREXプラットフォーム内でBCBが発行するホールセールDREXで決済されるようになる。DREXは、従来の金融取引と革新的な金融取引のコストを削減し、最終的には金融の民主化を支援する。 BCBの役割：金融・財政政策面への影響拡大。 ・当局が観測可能なデータを改善することで、政府による政策実施がより多くの情報に基づくことを可能にする。 ・金融・財政政策の実行の一部を自動化し、データベースに含まれる情報を自動的な方法で条件とできる（従前の支払金利が主な手段であることと対照的）。 【便益】 • スマートコントラクトが与信枠のルール遵守を自動的にチェックし、資金の適切な使用を保証することで、検証コストを削減する。 • CBDCは市民にとってより安価で使いやすい外国為替サービスを生み出す可能性がある。 • トークン化プロセスは、企業が取引を行うために保持する必要のあるデータ量を最小限に抑えようとするものであり、取引コストの低減、透明性の向上、流動性、効率性、代替資本源へのアクセス、分散化など、幅広いメリットを提供することができる。 • 公共・政府系を問わず、様々な台帳を流動的かつ低コストで相互運用可能にすることで、人々は、サービスのコスト削減、プレーヤー間の競争力強化、低所得層の顧客取り込み拡大といったメリットを享受できるようになる。 • ブロックチェーンの相互運用性を促進することで、競争を刺激し、コストを削減し、規模の経済を可能にし、利用者の利便性を高めるので重要である。 • 相互運用性の促進は、国の経済の資産の可視性を高め、暗号資産に積極的な世界中の投資家が国家金融システムに資本を拠出できるようにすることになり、利用者の利便性を高め、国の経済の資産への資本供給を増加させる。また、暗号通貨を利用しているユーザーの利便性も向上する。 • 外国為替に関しては、プール内の資産間の交換は中央集権化されたオーダーブックを必要とせずに行われ、外部市場からの供給者への依存を大幅に減らすだけでなく、ブロックチェーンで取引される資産に流動性を提供するプロセスを民主化し簡素化する。また、こうした取引所の流動性は分散型エージェント（裁定取引）からも把握できるため、中央集権的な機関にのみ依存する必要はなく、こうしたサービスを提供する機関の為替レートエクスポージャーのリスクも軽減される。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
DREXプロジェクト	【リスク】 1. 二重支出のリスク 　オフライン取引とオンライン取引では全く異なるフレームワークが必要なため、実装が複雑となり、二重支出のリスクが生じる。 2. プライバシーおよび銀行秘密法に関連するリスク 　パブリックネットワーク上の取引履歴は誰でもアクセス可能であり、各取引に参加しているウォレットの公開鍵と結びついている。 　ウォレットの所有者の身元が暴露された場合、そのウォレットとやりとりした他の参加者の身元も連鎖的に暴露される可能性がある。 　このリスクは銀行秘密法に反し、システムの信頼性に直接影響を与える。 　パブリック・ブロックチェーンの限界により、銀行秘密保護法に関連するリスクの解決は難しい。 3. 価格ミスマッチの投資家のリスク 　ボラティリティの高い通貨に対する請求額と受け取った額に「ミスマッチ」が生じるリスク。これはAMMの運用に関連し、トークンが追加されてから流動性プールから引き出されるまでの価格差に起因する。 4. 商業銀行の仲介役喪失のリスク 　CBDCが商業銀行を仲介しなくなるのではないかという懸念が生じる。 補足説明：CBDCが金融取引の構造を変革するならば、商業銀行の伝統的な役割を再定義する可能性がある。これまで、消費者が支払いを行う際には、商業銀行が仲介者として機能してきたが、CBDCが普及すると、その仲介役が不要になる可能性があるため、商業銀行の存在意義が減少するのではないかという懸念が生じる。CtoC（消費者間）の直接取引が増えることで、商業銀行の役割が縮小するという見方もあり、商業銀行のビジネスモデルや機能が大きく変化する可能性がある。 5. 移行リスク 　即時グロス決済がCBDCのインフラに移行する場合、移行リスクが生じる。 補足説明：既存の決済システムと新しいCBDCインフラが同時に運用される期間中、これらのシステム間での相互運用性が確保されていないと、決済が遅延したり失敗したりする可能性がある。システム間でデータフォーマットやプロトコルが異なる場合、情報の伝達や処理にエラーが生じることがある。 6. 変動損失のリスク 　AMMの報酬は価格差の関数であるため、流動性供給者には変動損失のリスクが生じる。 7. トークン価値の不確実性リスク 　トークンの価値が不確実になると、所有者に金銭的損失が生じる可能性がある。 　ステーブルコインでも為替リスクが存在する。

プロジェクト名	プロジェクト概要
DREXプロジェクト	8. ブロックチェーン運用リスク デジタル資産の保有者は、以下のリスクにさらされる： サイバー攻撃 カストディリスク（資産の紛失、アクセス制限、盗難、秘密鍵の盗難） ブロックチェーンの可用性障害 9. 金融政策コントロール喪失のリスク パブリックネットワークの利用により、CBDCと他のトークンの相互運用を管理するプロセスが複雑化する。その結果、金融政策のコントロールを失うリスクがある。 10. ブリッジ使用に伴うリスク ブリッジの発展途上性により、以下のリスクが存在する (i) コードの欠陥によるスマートコントラクトへの影響と資金損失の可能性 (ii) ソフトウェア障害や攻撃による技術的リスク (iii) ブリッジ運営者による検閲リスク (iv) ブリッジ運営者による資金盗難のカストディアル・リスク 11. オラクル問題に関連するリスク オラクルの問題が発生すると、スマートコントラクトのセキュリティ障害やプロジェクトの実行不可能につながる可能性がある。 リスクの詳細： (i) 情報セキュリティリスク（不正確な情報や虚偽の情報） (ii) データ更新の遅延リスク (iii) オラクル管理組織の評判リスク

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
DREXプロジェクト	【リスク軽減策】 1. 二重支出のリスク軽減策 オフラインとオンラインのフレームワーク間の統合や相互運用性の向上を図る。 二重支出を防止するための厳格な検証プロセスやセキュリティプロトコルを導入する。 2. プライバシーおよび銀行秘密法に関連するリスク軽減策 プライバシー保護技術（例：ゼロ知識証明、匿名化プロトコル）を採用する。 パーミッションド・ブロックチェーンを利用し、アクセス制御を強化する。 KYC/AML手続きを徹底し、データ漏洩防止策を実施する。 3. 価格ミスマッチのリスク軽減策 価格変動リスクをヘッジする戦略を導入する。 ボラティリティの低い通貨や資産を選択する。 リアルタイムで価格をモニタリングし、適切なタイミングで取引を行う。 4. 商業銀行の仲介役喪失のリスク軽減策 商業銀行がCBDCの流通や管理において新たな役割を担う仕組みを構築する。 商業銀行の付加価値サービスを強化し、エコシステム内での重要性を維持する。 5. 移行リスクの軽減策 既存の決済システムとCBDCインフラ間の相互運用性を確保するための標準化を推進する。 移行期間中のテストとモニタリングを徹底し、問題の早期発見と解決を図る。 6. 変動損失のリスク軽減策 流動性供給者に対するリスク教育と情報提供を行う。 インパマネントロスを最小化するアルゴリズムやAMMモデルを採用する。 リスクをカバーする保険商品やヘッジ手段を提供する。 7. トークン価値の不確実性リスク軽減策 トクンの裏付け資産や発行体の信頼性を透明化する。 為替リスクをヘッジする金融商品を活用する。 信頼性の高いステーブルコインを選択する。

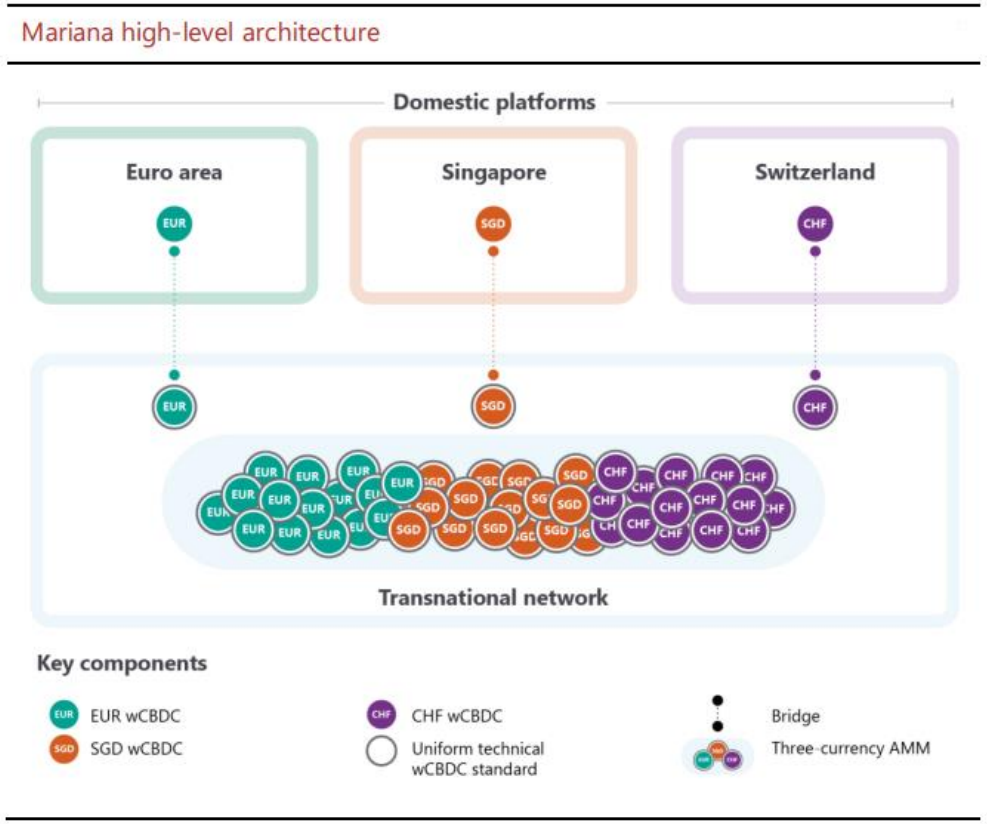
５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
DREXプロジェクト	8. ブロックチェーン運用リスクの軽減策 強固なセキュリティ対策（ファイアウォール、暗号化、侵入検知システムなど）を実施する。 資産の安全な保管のために信頼性の高いカストディサービスを利用する。 マルチシグネチャやハードウェアウォレットなど、秘密鍵の保護手段を強化する。 ブロックチェーンネットワークの冗長性と可用性を高める。 9. 金融政策コントロール喪失のリスク軽減策 規制当局や中央銀行が相互運用性の標準化プロセスに関与し、適切なガバナンスを確立する。 金融政策の実効性を維持するための技術的・制度的な仕組みを導入する。 10. ブリッジ使用に伴うリスク軽減策 ブリッジのスマートコントラクトコードを第三者機関によるセキュリティ監査を実施する。 信頼性の高いブリッジや成熟したプロトコルを選択する。 分散型ブリッジを採用し、中央集権的なリスクを軽減する。 11. オラクル問題に関連するリスク軽減策 複数のオラクルソースを利用し、データの正確性と信頼性を確保する。 オラクルデータの更新頻度を向上させ、リアルタイム性を高める。 オラクル管理組織の透明性とガバナンスを強化する。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
Project Mariana	Ethereum	Cross-border exchange of wholesale CBDCs using automated market-makers Final report	BIS Innovation Hub	2023年9月	【概要】 現在進行中の本プロジェクトでは中央銀行が中央銀行デジタル通貨（CBDC）を発行した世界を想定し、外国為替（FX）取引と決済のあり方を探っている。分散型金融（DeFi）のアイデアやコンセプトを取り入れ、自動マーケットメイカー（以下、AMM）がFX取引と決済を簡素化できるかどうかを研究し、市場効率の向上と決済リスクの低減を目指している。 【プロジェクト参加者】 BIS Innovation Hub (BISIH), Bank of France, Monetary Authority of Singapore, Swiss National Bank 【目的】 CBDCを使用したクロスボーダー決済プロセスの改善 【便益】 AMMは、将来のトークン化されたFX市場の輪郭を示し、多くの潜在的なメリットをもたらす。これには、FX取引のシンプルで自動化された執行のサポート、通貨範囲を広げるオプションの提供、決済リスクの排除、透明性の実現などが含まれる。 【リスク】 ホールセールCBDC（以下、wCBDC）が週7日、1日24 時間利用可能になることで、中央銀行にとっては、異なる形態の中央銀行マネー間で一貫した報酬を確保するなど、運用の複雑性が増す可能性がある。さらに、本PoCは、中央銀行が必ずしもプラットフォームを所有・管理することなく、wCBDC を管理できることを実証しているが、wCBDC スマートコントラクトは新たな脆弱性をもたらす可能性がある。具体的には、新しいタイプのセキュリテ ィ・リスクが発生する可能性があり、徹底的な検証が必要である。	本プロジェクトにおけるAMM は、FX取引の価格設定と自動実行、 即時決済を可能にするアルゴリズムを使用して、仮想のユーロ、シンガポール ドル、スイス フランの wCBDC をプールする。

出典：https://www.bis.org/publ/othp75.pdf

プロジェクト名	プロジェクト概要
Project Mariana	【研究内容】 • プロジェクト・マリアナの主な目的は、AMMに基づく銀行間FX市場を備えた、1日24時間、週7日稼動のwCBDC エコシステムの PoCを構築することで、AMMとwCBDCの両方を備えた、スポットFXのグローバル・インターバンク市場の概念実証（PoC）を実施したもの。新たなアプローチが既存の銀行間FXプロセスを簡素化できるかどうかを検証する。またこのアプローチが、透明性の向上と決済リスクの低減を通じて、クロスボーダー決済の強化に貢献できるかどうかも検証する。 • この目的のため、特に (i)wCBDC間の相互運用性のための共通技術標準、(ii)異なるネットワーク間の wCBDC 送金のためのいわゆるブリッジ、(iii)FX 取引と決済のための AMM の3つの主要な構成要素をテストする。 • 本プロジェクトは、wCBDC のアレンジメントと分散型台帳技術（DLT）プラットフォームを利用したクロスボーダー取引とFX 取引の実現可能性を検討するこれまでの研究（Bech et al (2023), BISIH et al (2022b) and BISIH (2023)）を拡張したものである。 • この実験では、仮想的なユーロ（EUR）、シンガポール・ドル（SGD）、スイス・フラン（CHF）のwCBDCを含む商業銀行間のスポットFX取引の取引と決済に注目している（図1-5-6参照）。 • 特に、このプロジェクトでは、プールで利用可能な流動性の量と、事前に定義されたアルゴ リズムのパラメータ化が、市場の流動性（つまり、wCBDC同士の取引のしやすさ）にどのような影響を与えるかを探ろうとした。 • これら2つの目的は、2つのユースケースにマッピングされる。ユースケース 1 は、AMMにおけるwCBDCを使ったFX取引に焦点を当てたものである。ユースケース 2 は、FX取引を促進するための市中銀行による流動性提供を検討する。 図1-5-6　PoCのアーキテクチャ 

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
Project Mariana	【研究結果】 • 第一に、wCBDCはスマートコントラクトとして実装され、中央銀行が基礎となるプラットフォームを直接操作または制御する必要なく、wCBDCを管理することを可能にする。wCBDCの設計はパブリック・ブロックチェーン分野のベスト・プラクティスに準拠しており、広く使われている標準（ERC-20など）をベースにしており、アップグレードも可能である。 • 第二に、ブリッジは、トークン化されつつあるエコシステムにおいて、より広範な相互運用性を確保するメカニズムとして機能する可能性がある。ブリッジは、PoCで実装されているように、人手を介することなく、国内のプラットフォームと国境を越えたネットワークとの間で wCBDCをシームレスかつ安全に移転することを可能にする。ブリッジの設計は、中央銀行によって管理されるオンチェーン（ブリッジスマートコントラクトなど）およびオフチェーン（ブリッジスマートコントラクト間の通信など）のインフラを通じて、コントロールとセーフガードを特徴とし、弾力性を確保する。 • 第三に、プロジェクト・マリアナでテスト・調整されたAMMは、選択されたFXグローバル・コード（FXGC）の原則に基づく要件を満たしている。AMMは、将来のトークン化されたFX市場の輪郭を示し、多くの潜在的なメリットをもたらす。これには、FX取引のシンプルで自動化された執行のサポート、通貨範囲を広げるオプションの提供、決済リスクの排除、透明性の実現などが含まれる。しかし、AMMの利用には流動性の事前調達が必要であり、AMMの採用は、今日のFX市場で利用されている事後調達（繰延ネット決済）とは大きく異なる。 • プロジェクト・マリアナのPoCは、wCBDCを利用したホールセールFX取引におけるAMMの潜在的な利点と課題を理解するための第一歩であった。しかしながら、サイバー攻撃はブロックチェーンやDeFi技術の脆弱性を繰り返し明らかにし、しばしば関係者に多大な損害を与えており、様々な側面についてさらなる研究が必要である。 • トークン化やDeFiには潜在的な利点があるが、セキュリティ上の疑問点を徹底的に調査する必要がある。 • より広義には、将来的にはプロジェクト・マリアナを3つの分野に拡張することができるだろう。第一に、技術的な実現可能性だけでなく、ホールセールFX取引におけるAMMの既存の取り決めに対する商業的な実現可能性を明らかにする必要がある。このような検討を可能にするには、FX市場の関係者間の協力が必要であろう。第二に、トークン化によって、金融政策の実施に関する疑問が生じる可能性がある。具体的な疑問（例えば、wCBDC の報酬）から、非常に広範な疑問（例えば、DeFi のアイデアやコンセプ トに基づく金融政策手段）まで様々である。第三に、ステーブルコイン、トークン化された預金、トークン化された債券や証券などの金融商品を含む可能性のある、より広範なトークン化されたエコシステムにおける中央銀行とwCBDCの役割を理解するためには、さらなる研究が必要である。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
JPM Coin	許可型ブロックチェーン/Quorum	DEPOSIT TOKENS A foundation for stable digital money	Oliver Wyman, Onyx by J.P. Morgan,	2022年	【概要・目的】 JPM コインは、デポジット・トークンとして、米ドルに1:1で裏付けられている。2020年にローンチされ、JPモルガンの機関投資家の顧客間における即時グロス決済に対応する。 本文献では、JPMコインをデポジットトークンのユースケースとして、そのメリット、ステーブルコインや CBDC との区別に焦点を当てる。そうすることで、デポジット・トークンを異なるタイプのデジタルマネーとして焦点を絞った議論を提供し、様々な形態のデジタルマネーに関する現在進行中の政策議論に貢献し、業界と規制当局が将来のデジタルマネーの展望において商業銀行が果たす役割を理解するために先を見据えている関係者に情報を提供することを意図している。 【プロジェクト参加者】 JPモルガン 【研究内容】 世界のデジタルマネー事情、デポジット・トークンの使用例。政策的考察 【研究結果】 デポジット・トークンは、銀行の既存の預金取り扱い業務に根ざしたものである。伝統的な銀行システムとブロックチェーンの間に生産的な連携を生み出すためには、設計においても規制においても、それらの伝統的なシステムの延長として存在しなければならない。	JPモルガンのグローバル・ペイメント・ヘッドであるタキス・ゲオルガコプロス氏は2023年10月26日、JPMコインで1日あたり10億ドル以上の取引を処理していると発言している。 ※JPMの決算事業全体では1日あたり10兆ドル近く処理しているため、約1000分の1に相当する。

出典：https://www.jpmorgan.com/onyx/documents/deposit-tokens.pdf
https://www.coindesk.com/business/2023/10/26/jpmorgan-handles-1b-transactions-daily-in-digital-token-jpm-coin-bloomberg/

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
JPM Coin	ブロックチェーンベースのデポジットとは、ブロックチェーンに記録された指定金額に対する認可された預金機関に対する預金請求を指す。これは、支払い、デジタル資産間の取引の決済に使用される新しい形式で記録された既存の預金の経済的同等物であり、一般的にはブロックチェーン台帳上の価値の保存および交換手段として機能する。このようにブロックチェーン技術を適用することで、商業銀行のお金で行われた支払いは、プログラム可能性、即時かつアトミックな取引決済、および取引状況に関する透明性の向上の恩恵を受けることができる。これらの機能は、流動性管理と国境を越えた支払いにおける一般的な問題点に対処するのに役立つ。

表1-5-7　ブロックチェーンベースのデポジット、ステーブルコイン、CBDCの比較

	ブロックチェーンベースのデポジット	ステーブルコイン	CBDC
一般的な発行体	商業銀行	銀行以外の民間団体	中央銀行
例	JPモルガンによるSGDデポジット・トークン JPMコインシステムのブロックチェーン預金口座	CircleとCoinbaseによるUSDC テザーによるUSDT PaxosとバイナンスによるBUSD	デジタル元（パイロット延長） スウェーデン・Eクローナ（パイロット） デジタルユーロ（調査）
採用状況	JPMコイン・システム、取引量増加で本稼働 デポジット・トークン・プロジェクトは、一般的に初期のパイロット段階にある。	最初の主要なステーブルコインが発行された2014年以降、時価総額は1400億米ドル以上（2022年11月時点）	90%以上の中央銀行がCBDCを調査していると言われているが、実際のプロジェクトはまだ初期のパイロット段階である。
裏付け資産	通常の預金と同様、発行体に対する債権	1:1 発行体が保有する資産を充足するため通常はHQLA(High Quality Liquid Assets)として保有される償還金	中央銀行のバランスシート
規制監督	他の規制銀行預金と同様の監督・監視の対象となる。	規制の枠組みは生まれつつあるが、ほとんどの市場に規制の枠組みはない	国家機関が直接確保し、管理する
リスク 経営慣行	流動性、資本、リスク管理の最低義務要件に従う。規制当局による 銀行の内部リスク管理慣行に従う	統一されたリスク管理フレームワークがない 発行体の内部リスク管理慣行に従う	
緊急保護	既存の銀行バランスシートの強さ 中央銀行の緊急資金源へのアクセス 財政難を克服するための解決および回復計画	準備資産の清算 従来の破産法に基づく解決	

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
JPM Coin	【便益】 • 銀行システムに統合されたデポジット・トークンは、手作業によるソリューションを自動化し、手作業による介入なしに複雑な取引ロジックを可能にし、人為的なエラーや遅延のリスクを軽減することで、プログラマブルになることで新たなメリットをもたらす。このような自動化は、決済の実行だけでなく、流動性や担保の管理も効率化する。 • 預金トークンのメリットは、他の銀行が発行する預金トークンやトークン化されていない金銭形態との融通性を高めるような設計を選択することで最適化できる。 • 顧客の流動性資金ニーズを簡素化し、次世代の企業財務サービスを提供する。JPM コインは、支払いレールおよび預金口座台帳として機能する許可システムであり、JP モルガンの参加顧客はシステム内で JP モルガンに預金されている米ドルを転送できるようにすることで、流動性資金の移動が容易になり、適切なタイミングでの決済できる。DVP、PVP、マシンtoマシン支払いなどを国境を越えてサポートする。 • クロスボーダー決済は、共有台帳上で情報と価値を統合することで最も顕著な効果が期待できる分野である。多通貨のCBDCがコストを80%削減すると見積もっている。預金トークンも手数料、決済時間、カウンターパーティーリスクを削減することで、CBDCと同様の利益を引き出す可能性がある。 • 銀行システムに統合されたデポジット・トークンは、手作業によるソリューションを自動化し、手作業による介入なしに複雑な取引ロジックを可能にし、人為的なエラーや遅延のリスクを軽減することで、決済の実行だけでなく、流動性や担保の管理を効率化する。 • トークン化された資産マーケットプレイスはアトミックあるいは同時にほぼ瞬時に決済されるため、取引相手が失敗したり資産を引き渡せなかったりして、取引の一部が決済されないリスクが排除される。 • 金融安定：従来の決済システムよりも効率的で安全な決済システムを提供することで、金融システム全体の安定性を向上させる可能性があると考えている。分散型台帳技術（DLT）に基づいており、これは取引の透明性とトレーサビリティを向上させるのに役立つ。 • 利用者保護：強力なセキュリティ対策を備えており、不正アクセスや盗難からユーザーを保護する。ユーザーのプライバシーを保護するために設計されている。ユーザーに透明性とコントロールを提供するように設計されている。 【リスク】 • デポジットスキームを使い、伝統的な商業銀行預金に適用されている既存の慣行や規制を活用することで、ステーブルコインが持つリスクの軽減を図っている。 • 従来の預金と同様に、デポジットトークンは発行預金取扱機関に対する債権である。従って、非ブロックチェーン方式で記録された預金の安全性と健全性を確保するために、今日、 預金取扱銀行に課せられている流動性要件やリスク管理基準に従うべきである。 • 人間の直接的な関与を減らすことは、ソフトウェアのバグによる気づかないエラーの可能性や制限などのリスクももたらす。スマート・コントラクトはレビューと監査を受け、予想される問題は修正されるべきである。今日の銀行機関は、銀行サービスを提供する過程で、高度なソフトウェアを定期的に開発・採用しており、その実務はリスク管理委員会が監督する技術リスク管理基準の対象となっている。そのような専門知識とリスク管理慣行には、他の銀行が開発したソフトウェアや銀行が採用したソフトウェアと同様に、プログラマビリティ・ソリューションの強固な開発のための専門知識とリスク管理慣行が必要である。 • 償還などのオンチェーン活動のリアルタイムの透明性は、多額の償還を行うユーザーの活動を表示することで償還リスクの認識を悪化させ、他のユーザーの同様の償還が実施されないことへの懸念と取付行動（ラン・リスク）を誘発する可能性がある。 • ステーブルコインのブリッジングとラッピングは、通常、第三者が作成したスマートコントラクトによって行われてきたが、これには運用リスクと技術リスクが追加される。

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
DTCC Project Ionプラットフォーム	許可型ブロックチェーン/Corda	BUILDING THE SETTLEMENT SYSTEM OF THE FUTURE	Murray Pozmanter Head of Clearing Agency Services and Global Business Operations	2021年9月	【概要・目的】 中央清算機関（Counterparty Clearing）が提供する効率性への支持を含め、将来の決済システムに対するデポジトリー・トラスト・クリアリング・コーポレーション（以下、DTCC）のビジョンを示す。また、DTCCが提供するDLTであるProject Ionの情報を提供する。 Project Ionは、清算・決済に新たな効率性をもたらす技術として分散型台帳技術（DLT）を活用し、清算・決済機能を導入するもの。 【プロジェクト参加者】 DTCCの子会社である、ナショナル・セキュリティーズ・クリアリング・コーポレーション（NSCC）およびデポジトリー・トラスト・カンパニー（DTC） 【研究内容】 DLTにおける清算・決済の効率性の追求 【研究結果】 Project Ionでは、T+1またはT+0環境での決済がDLTで有効なユースケースになりうることを実証した。 DTCCは2020年半ばからDLTのユースケースとしてProject Ionの概念実証をテストしている。2021年に機能を拡張したプロトタイプでは、DLTノードの採用、APIインターフェース、ユーザーインターフェースなど、複数のインターフェースをパイロットユーザーに提供するもの。戦略的ロードマップの主要コンセプトにおいて、決済の最適化や決済の高速化を置いている。特にT+0決済サイクルを中心にモデル化をすすめている。 複数のDTCCの顧客がプロトタイプに参加し、DTCCのコアとなる清算・決済プロセスとワークフローを強化するためのDTCCの見解を形成するためのフィードバックを提供した。	Project Ion は、DTCC (Depository Trust & Clearing Corporation)における既存の決済サービスの代替的なサービスとして提供される株式決済基盤である、ピーク日において1日16万件の処理を行ったとしている。ブロックチェーン関連技術としては、Corda DLTが用いられている。2024年3末現在も、MVP(minimum viable product)として、パイロットが稼働している。 出典：DTCC Consulting「DTCC’s Project Ion platform」

出典：https://www.dtcc.com/dtcc-connection/articles/2021/september/16/building-the-settlement-system-of-the-future

５　伝統的金融機関が関与するトークナイゼーション関連プロジェクト

プロジェクト名	プロジェクト概要
DTCC Project Ionプラットフォーム	【便益】 決済時間が短縮されることで、市場リスクと必要証拠金が減少し、企業はそのリソースを他の方法で活用できるようになる。 ●証拠金の削減：ブローカー／ディーラーにとって、T+1への移行は必要証拠金と担保の大幅な削減につながる。現在、システムのカウンターパーティ・デフォルト・リスクを管理するために、毎日平均134億ドル以上の証拠金が保有されている。決済サイクルの短縮は、リスクベースの証拠金とプロシクリカルな影響のバランスを改善するのに役立つ。DTCCが行ったリスク分析とリスクモデルのシミュレーションによると、NSCCの証拠金のうちボラティリティ部門は、現在の処理を前提とし、顧客の行動に他の変更がない場合、T+1に移行することで約41%削減できる可能性がある。過去1年間、ボラティリティ・コンポーネントはNSCCの証拠金総額の約60%を占めている。特に、市場のボラティリティが高いときには、この金額が大幅に大きくなる。 ●リスク削減：決済サイクルが短縮されれば、業界に必要な証拠金が削減され、投資家のコストが低下する一方で、T+1の実現に必要なシステム面やプロセス面の改善により、市場のレジリエンスも強化される。T+1への移行は、システミック・リスク、オペレーショナル・リスク、流動性ニーズ、バイサイドのカウンターパーティー・エクスポージャー、ブローカー間のカウンターパーティー・リスクの低減など、多くのメリットをもたらす。

６　金融セクターにおけるトークナイゼーションのインパクト

- 以下に、伝統的金融機関の貸借対照表における資産と負債と、ブロックチェーン関連技術を用いたユースケースをマッピングした図を示す。
- 将来的には、伝統的金融機関がこれらのデジタル資産・負債を積極的に取り扱う機会が増加し、それに伴い貸借対照表へのインパクトがより一層拡大する可能性がある。

図1-6-1　貸借対照表とブロックチェーン関連技術

表1-6-2　デジタルアセットの概況

デジタルアセット	概況
ステーブルコイン	主なステーブルコイン合計（USDC、USDT、BinanceUSD、DAI等）の2023年における時価総額は概ね1200億ドルを越えて推移していた。
デポジットトークン	発行額は少ないが、JPモルガンによるJPMコインなど、実用化に向けた動きがある。
デジタル社債	国内では2023年に13件150億円の発行があった。
デジタル受益証券	国内では2023年に29件約1000億円の発行があった。

７　金融セクターにおけるトークナイゼーションの性質

- 国内において、伝統的金融機関が取り扱っているトークンはほぼすべてパーミッションドチェーンで発行されている。一方、国外では、イーサリアムのようなパーミッションレスチェーンを用いて発行された例（BlackRockのBUIDLファンドなど）がある。また、暗号資産交換業者が取り扱うトークンの多くは、主にパーミッションレスチェーンで発行されている。
- 伝統的金融機関が取り扱うトークンと暗号資産交換業者が取り扱う暗号資産では、取引の性質において異なる点が多い。

表1-7-1　被規制金融機関が取り扱うトークン取引の性質による違い

態様	暗号資産交換業者が取り扱うパーミッションレスチェーン	伝統的金融機関が取り扱うパーミッションレスチェーン	伝統的金融機関が取り扱うパーミッションドチェーン
主なトークン	暗号資産、ステーブルコイン	セキュリティトークン、ステーブルコイン	セキュリティトークン、ステーブルコイン
KYC	アドレス（公開鍵から生成される）だけでは本人かどうかを証明できない。 暗号資産交換業者はKYC済みの顧客属性とアドレスを紐づけて、継続的に顧客を管理している。	アドレス（公開鍵から生成される）だけでは本人かどうかを証明できない。 伝統的金融機関はKYC済みの顧客属性とアドレスを紐づけて、継続的に顧客を管理している。	参加者が許可されたユーザーに限定されているため、KYCで得られた顧客情報が公開鍵証明書のように信頼できる身元保証の役割を果たしている。
トークンの移動制限	投資家が管理する個人ウォレットにトークンを移動できる。個人ウォレットから、KYC未済のウォレットにトークンを移動できる。 アドレス単位でブラックリストにもとづいて制限可能。	原則として、投資家が管理する個人管理ウォレットにトークンを移動することはできないよう設計する必要性がある。 トークンの管理は伝統的金融機関に委ねられる。	
公開鍵証明書に対する失効権限	公開鍵証明書（公開鍵が本当にその人に属していることを保証するもの）の仕組みが存在しないため、失効権限も存在しない。 ただし、ソーシャルリカバリーウォレットに代表されるように、スマートコントラクトによって公開鍵証明を行う仕組みを導入することで、公開鍵を失効させたり、新しい鍵ペアで置き換えたりできる方法は存在する。		伝統的金融機関が失効権限を有している。

出典：https://decrypt.co/222694/blackrock-ethereum-fund-buidl

８　総括

１章１では、「ブロックチェーン関連技術と分散型金融システムの登場と普及」として、暗号資産の誕生からはじまり、ブロックチェーン関連技術の応用的活用方法として、分散型金融システムで多くの取引がなされている状況について紹介した。

１章２では、「分散型金融の特性と伝統的金融との比較」として、伝統的金融では、取引主体はKYC済であり、主なサービス提供者は業規制のもと、認可を受けた金融機関が担っており、当局等により、監督下に置かれているが、分散型金融（とくに誕生初期）では、取引主体が不明瞭であり、主なサービス提供者がDAOである点など、相違点について解説した。

１章３では、「分散型金融に対する監督のあり方の見直し」として、分散型金融におけるハッキングなどの事故増加を受け、業規制を検討する動きなどを紹介した。

１章４では、「分散型金融の事例紹介」として、利用者保護などを目的とした取り組み事例を紹介した。

１章５では、「伝統的金融機関が関与するトークナイゼーションの検証プロジェクト」として、伝統的金融機関や規制当局等によるトークン化や分散型金融に対する金融安定や利用者保護等に関連する研究内容を紹介した。

１章６では、「金融セクターにおけるトークナイゼーションのインパクト」として、金融機関のBSに計上されうるデジタルアセットの市場動向を紹介し、トークン化の拡大傾向が続けば、伝統的金融機関に対するインパクトも拡大する可能性を示唆した。

１章７では、「金融セクターにおけるトークナイゼーションの性質」として、暗号資産交換業者をとりまく状況と異なる傾向があることを示した 。

本章では、~~このように、~~金融セクターにおけるトークナイゼーションの動向や、分散型金融関連システムにおける金融規制に対応しようとする試みについて紹介してきた。トークナイゼーションや分散型金融関連システムについて、被規制金融機関が管理し、規制当局等が監督するためには、仕組みの理解と、より適した管理・監督手続きを模索すべき必要性があるであろう。

そこで、2章では、ブロックチェーン関連技術における規制当局によるSupTechや被規制金融機関によるRegTechについて、検討事例を調査する。

第２章　ブロックチェーン技術等のRegTech/SupTechへの活用可能性

第２章 ブロックチェーン技術等のRegTech/SupTechへの活用可能性

本文書において、第２章に登場する主な専門的な用語について、以下のとおり定義する。

用語	定義
埋め込み型監督（Embedded Supervision）	分散型台帳に監督機能を組み込むことで自動的に取引や帳簿データを監視する技術をいう。これにより、企業が能動的にデータを収集、検証、提供する必要性が減ることが期待されている。 当定義はBISが2019年9月に公表した「Embedded supervision:how to build regulation into decentralised finance」を参考にした。 本文書では、埋め込み型監督の対象として、被規制金融機関が自ら主管する分散型金融システムおよびその関連システムにコンプライアンス機能を組み込む場合や、規制当局等が監督したい分散型金融システムに関連するシステムに監督機能を組み込む場合を想定した。
監督ノード（Supervisory Node）	監督ノードは、金融機関の取引内容を常時監視するノードである。本文書では、規制当局等自らがノードを主管する場合を想定した。
SupTech	規制当局等によって利用される、規制業務を支援する技術をいう。 紙ベースの書類や手作業によるデータ分析などが中心である従来の監督・監査業務に対して、SupTechは、規制当局等がAI、ビッグデータ、クラウドコンピューティング、ブロックチェーンなどのIT技術を活用することで、これらの業務を効率化・自動化・高度化することを目的としている。
RegTech	被規制金融機関によって利用される、規制・報告義務等の法令遵守をサポートする技術をいう。 紙ベースの書類や手作業によるデータ分析などが中心である従来の規制・報告義務等の法令遵守対応業務に対して、RegTechは、被規制金融機関が、AI、ビッグデータ、クラウドコンピューティング、ブロックチェーンなどのIT技術を活用することで、これらの業務を効率化・自動化・高度化することを目的としている。

本文書では２－１において、当局等の検証プロジェクトの中から、SupTechとしての監督ノードや、 SupTechあるいはRegTechとしての埋め込み型監督に関する先行事例や文献等を調査する。

次に２－２において、IOSCOの“同じ活動、同じリスク、同じ規制・規制結果 ”という指導原則に照らし、ブロックチェーン技術を用いている分散型金融と規制要件を満たした伝統的金融のRegTechに相当する機能を対比して紹介し、分散型金融におけるRegTechの意義について考察する。

１　当局等が関与するRegTech/SupTechの検証プロジェクト

第１章では、金融セクターにおけるトークナイゼーションの動向や、分散型金融関連システムにおける金融規制に対応しようとする試みについて紹介してきた。トークナイゼーションや分散型金融関連システムについて、被規制金融機関が管理し、規制当局等が監督するためには、仕組みの理解と、より適した管理・監督手続きを模索する必要性があるであろう。

そこで、２－１において、当局等の検証プロジェクトの中から、SupTechとしての監督ノードや、SupTechあるいはRegTechとしての埋め込み型監督に関する先行事例や文献等を調査する。

- 本章において調査対象としたプロジェクトは以下のとおりである。
  - A New Use Case: A Supervisory Node（ボストン連銀）
  - Embedded supervision: how to build regulation into decentralised finance（BISワーキングペーパー）
  - The Use of Supervisory and RegulatoryTechnology by Authorities and RegulatedInstitutions（FSB）
  - “Decentralised” or “disintermediated” finance: what regulatory response?（仏ACPR）

１　当局等が関与するRegTech/SupTechの検証プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
ボストン連銀PoCプロジェクト	Ethereum, Hyperledger Fabric	Beyond Theory: Getting Practical With Blockchain	Federal Reserve Bank of Boston	2019年2月	【概要】 本文献はボストン連邦銀行が2016年から2017年にかけて実施してきた２種類のブロックチェーンの概念実証（PoC）に関する報告である。 【プロジェクト参加者】 ボストン連銀内の技術者チーム 【研究内容】 実際の導入ではなく技術を学ぶことを目的として、「各預金機関と連銀の総勘定元帳との調整業務」という具体的なユースケースの検討・実装を行った。そこから得られたブロックチェーン・プラットフォームを実装する際のポイントについてまとめた。 【研究結果】 （メリット・示唆） 1．プロジェクトの中で期待していた結果を、既存の技術とフレームワークを利用し、連銀内のチームのみで概ね実現できた。 （課題） 1．オープンソースコミュニティがボランティアベースであり、技術的なサポートが未成熟で、ドキュメントやQA対応が十分でなかった。加えて技術の進歩が早く、しばしば大規模なコード修正などの対応を迫られた。 2．Ethereumは基本的にプライベートな取引に対応しておらず、ユースケースに適さなかった。Hyperledger Fabricはプライベートなチャネルを設定することができるが、非常に複雑なネットワーク図になってしまう。 （今後） Hyperledger Fabricの新たなユースケースとして「監督ノード」が検討された。具体的な実証は実施されなかったが、Hyperledger Fabricの各プライベートチャネルの中心に監督ノードを設置する構成が検討されている。	ボストン連銀のWebサイトにおいて、本文献とともに、「分散型台帳技術の基礎を超えて、ボストン連銀がブロックチェーン プラットフォームが業務内の特定の機能の実行にどのように役立つかを理解するために学習を目的として、2つのユースケースを開発する。これらを本番環境に移行するつもりはない。このレポートでは、ユース ケース、採用したテクノロジー、および得られた洞察について説明する」旨の紹介文が掲載されている。

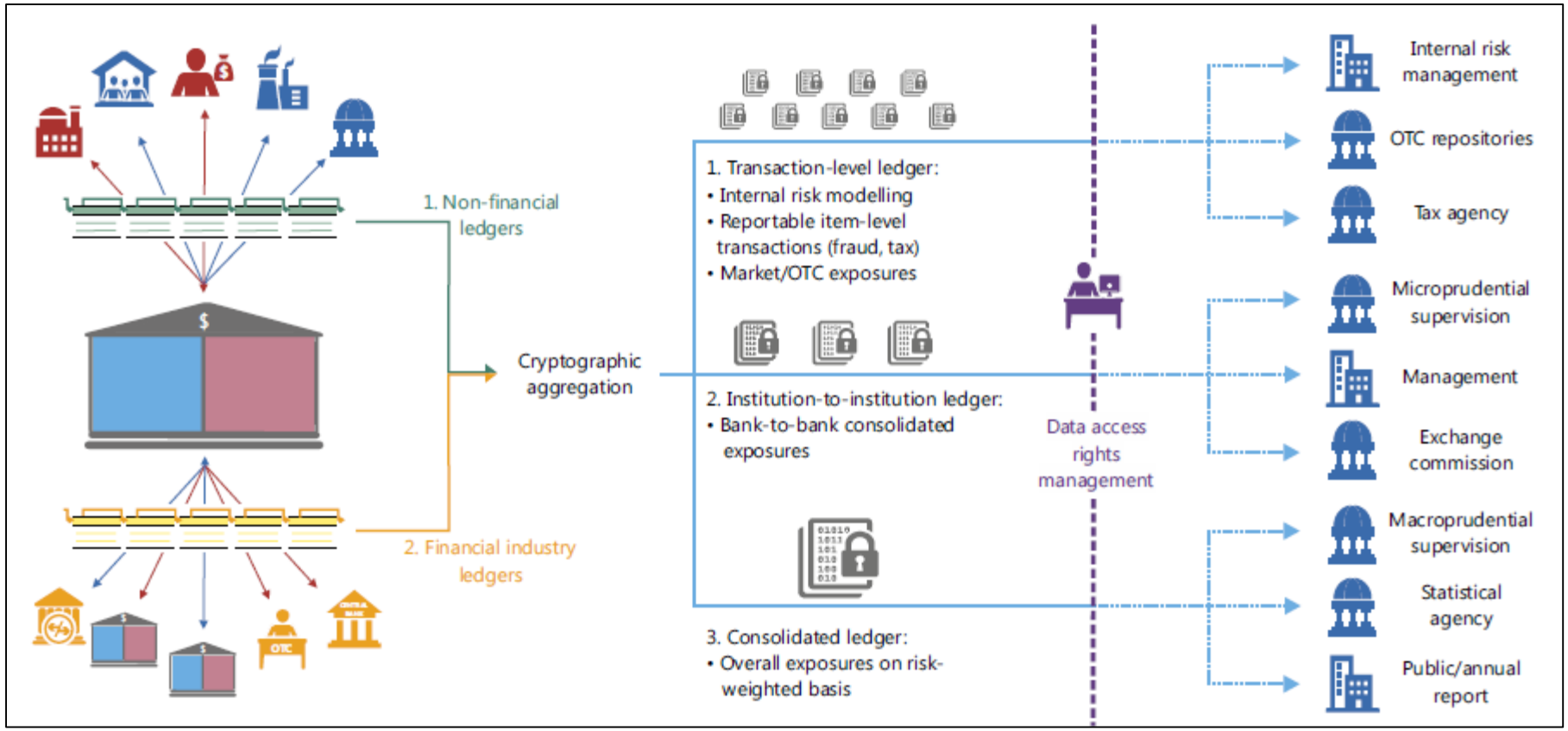
出典：https://www.bostonfed.org/publications/fintech/beyond-theory-getting-practical-with-blockchain.aspx

プロジェクト名	概要
ボストン連銀PoCプロジェクト	監督ノードは一般的な用語であり，監査役，決済ネットワ ークの規則執行者，データ報告機関など，FRB の規制監督者 としての役割を超えた多くの役割を含みうる。そのため、実験の中には、規制監督機関としての具体的な役割とは必ずしも結びつかない、より一般的なものもある。本プロジェクトでは、ブロックチェーン技術とスマートコントラクトのロジックが、人工知能や機械学習と組み合わされることで、どのようなことが実現できるのかについて以下の課題を認識している。 ●監督ノードはどのようなビジネス機能（監査、規制監督者、決済ネットワークのルール実施者）を果たすことができるか？ ●監督ノードはどのようなアーキテクチャ上の問題を引き起こすのか？ ●データへのアクセスを、規定の機能を果たすために必要なものだけに制限できるのか？ ●監視ノードが危険にさらされたり、ネットワークに運用上のリスクが生じたりする可能性はあるか？ ●複数のブロックチェーンプラットフォームが特定のビジネスプロセス（例：DVP）に利用される場合、監督ノードのアーキテクチャとパフォーマンスにどのような影響があるか？ ●監督責任を共有する姉妹監督機関が単一の監督ノード構造を開発できたとしたら、それはどのような新たなアーキテクチャ／技術的問題を提起するか？ ●民間決済ネットワークにおける悪意のある行為者を検出し、管理するために何ができるか。(これは連邦準備制度理事会(FRB)の役割を超えて、民間決済ネットワーク運営者のような規則執行を担う当事者により適切に適用されるかもしれない)。 ●不正はどのように検知できるのか？AIロジックでサポートされたノードによって共有ネットワークで検知できる場合、どのような対応が考えられるか？

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	概要	当研究に関連する記述など
BISの研究活動報告	分散型金融・分散型台帳一般	Embedded supervision: how to build regulation into decentralised finance	Raphael Auer	2019年9月（2022年５月改訂）	【概要】 本文献では、「埋め込み型監督」という新しい概念を提唱する。これは、分散型市場において、市場の台帳を自動的に読み取ることでコンプライアンスを監視する枠組みをいう。従来の法制度による規制とは異なり、分散型市場では経済的な合意に基づいてデータの信頼性が担保される。そのため、規制当局は、埋め込み型監督を実現するために、高度な技術的ノウハウと強い意志を持つ必要があると言えるだろう。 【埋め込み型監督の想定効果】 1.自動化による効率性向上 埋め込み型監督の基盤となる分散型台帳技術は、需要と供給のマッチングや価格発見といった市場取引の根幹を自動化できる。この技術を活用することで、取引所や店頭市場、さらには将来的には有価証券やデリバティブ取引までも自動化できる可能性を秘めている。 例えば、資産担保トークンを保有する銀行の場合、バーゼルIII資本基準への準拠を自動的に検証できるようになる。これは、分散型台帳における残高の所有権とリスクウェイトを計算することで実現する。同様に、トークンエコシステムでは、ステーブルコインの資産の裏付けを自動的に監視することも可能になる。 2.管理コスト削減 自動化された金融取引を監督することで、規制当局と金融機関双方にとって大きな負担となっているコンプライアンス管理コストを削減できる。 ３．決済リスクの低減 取引の自動化は、決済失敗に伴うオペレーショナルリスクを最小限に抑える効果も期待できる。 ４．データへのアクセス性向上 分散型台帳は、すべての基本的な取引データを自動的に記録する。埋め込み型監督を活用すれば、これらの取引データに容易にアクセスできるようになる。 埋め込み型監督は、分散型市場におけるコンプライアンスを確保するための革新的なアプローチと言える。自動化、コスト削減、リスク低減、データアクセス性向上といった様々なメリットをもたらす可能性があり、今後の発展に大いに期待が持てるだろう。	本文献における「埋め込み型監督」とは、分散型台帳に監督機能を組み込むことで、取引や帳簿データを自動的に監視する技術のことを指す。 「埋め込み型監督」は分散型台帳のメリットを享受することができ、規制当局による監督を効率化・高度化できる可能性がある（左記参照）。 さらに、本文献は重要なポイントとして、分散型金融システムが普及・拡大していく上で、「経済的ファイナリティ」（取引が確定し所有権が移転したとみなされること）の概念を根本的に定義しなおす必要があることを示唆している。 従来の金融システムでは、中央集権的な機関が取引の確定と所有権の移転を保証していた。しかし、分散型金融システムでは、そのような中央機関が存在しないため、経済的ファイナリティの概念を再定義する必要がある。本文献は、分散型金融システムにおける経済的ファイナリティの概念を明確化することで、より安全で効率的な金融取引を実現できると主張している。

出典：https://www.bis.org/publ/work811.htm

プロジェクト名	概要
BISの研究活動報告	【埋め込み型監督の原則】 埋め込み型監督について、以下をその利用の指針としている： ●埋め込み型監督は、効果的な法制度とそれを支える制度に支えられた全体的な規制の枠組みの一部としてのみ機能しうる。 ●埋め込み型監督は、経済的ファイナリティを達成する分散型市場にも適用できる。 ●埋め込み型監督は、経済市場のコンセンサスの中で、市場が自動的に監督されることにどう反応するかを考慮して設計される必要がある。 ●埋め込み型監督は、低コストのコンプライアンスを促進し、大企業と中小企業の公平な競争条件を確保すべきである。 【運用上の留意点】 規制当局・金融機関が埋め込み型監督を実際に運用していくインセンティブを得るために、以下のような観点から埋め込み型監督の運用面における注意点を視野に入れる必要がある。 1.　公平性：コンプライアンスコスト削減により大小の金融機関の競争条件を公平にすることを目指すべきである。 2.　限界費用の削減：各種統計や登記情報など、信頼できる公的情報へのアクセスを容易にすることでビジネスを行う際の限界費用を削減することを目指すべきである。 3.　分散型台帳そのものの限界：埋め込み型監督の技術的土台である分散型台帳にもセキュリティの脆弱性は存在する。分散型台帳の活用は標準的な取引や契約のプロセスを簡略化するに過ぎず、込み入った状況に陥った場合は従来の通り法的な手続きに頼る必要がある。 埋め込み型監督は、金融機関のコスト負担を軽減し、監督官に高品質なデータを提供する。ただし、台帳データの信頼性には法的保証が必要である。技術的には、暗号化技術を利用して、監督官が必要とするデータにのみアクセスできる仕組みを考慮すること。 【従来の研究との新規性】 従来の規制は既存の法体系に基づいているが、本文献では分散型市場の特性を活用して新しい監視フレームワークを提案している。経済的コンセンサスに基づく自動監視の可能性を具体的に探求した点が新規といえる。 【限界】 提案されたフレームワークは、分散型台帳の経済的信頼性を確保するために、法的基盤や運用支援機関に大きく依存する。また、監視が市場参加者に与える影響についてもさらなる研究が必要となる。 【潜在的応用】 本文献は、DeFi市場での規制遵守を簡素化することで、小規模金融機関や新規参入者にとっての市場アクセスを向上させる可能性を示唆している。また、台帳データの即時利用が可能になることで、より効率的な金融監視を実現しうる。

プロジェクト名	概要
BISの研究活動報告	埋め込み型監督は、ホールセール（図2-1-1、黄色のブロックチェーン）とリテールバンキング市場（同、緑色のブロックチェーン）の両方で分散型台帳を読むことによって、規制の遵守を検証することができる。監督当局はすべての取引レベルのデータにアクセスできる。あるいは、スマートコントラクト、マークル木、準同型暗号化、その他の暗号化ツールを使用することで、監督当局はそのようなミクロデータの選択された部分、あるいは機関対機関やセクター別エクスポージャーなどの関連する連結ポジションにのみ検証可能なアクセスができるようになるかもしれない。企業は関連するアクセス権を定義するだけでよく、データを収集、編集、提供する必要がなくなる。 図2-1-1　埋め込み型監督を用いたコンプライアンスプロセス 

プロジェクト名	概要
BISの研究活動報告	関連する分散所有台帳の貸借残高と関連するリスクウェイトを計算することで、自動的に検証することができる。このような計算は、報告期間末のコンプライアンスなど、ストック・ポジションに適用されるだけでなく、元帳ベースの仕組商品や契約債務のシミュレーションによるバリュー・アット・リスクの自動計算など、市場の変動に対するバランスシートのエクスポージャーのリアルタイム感度分析にも利用できる。同様に、「オンチェーン」担保付きステーブルコインの全資産の裏付けを自動的に検証することもできる。

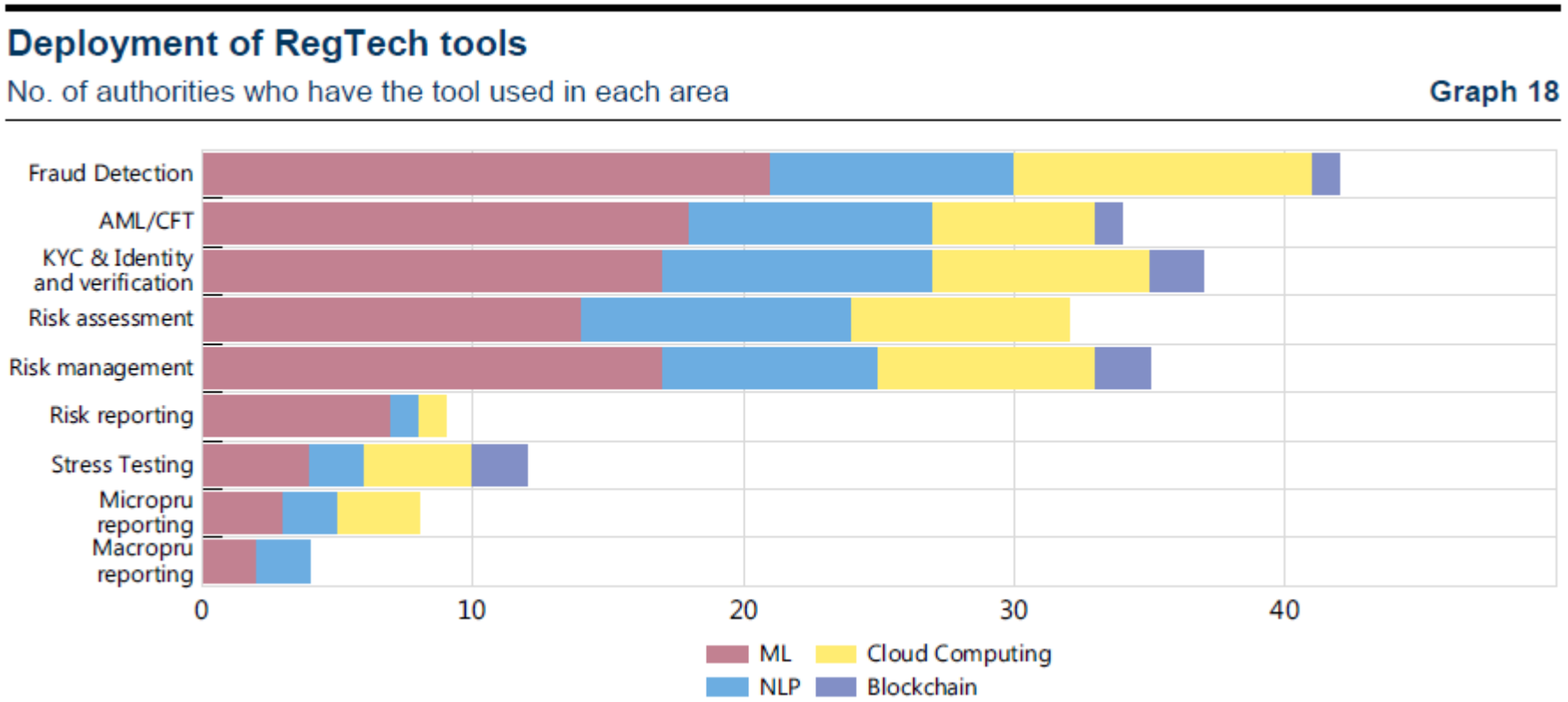
１　当局等が関与するRegTech/SupTechの検証プロジェクト

プロジェクト名	対象テクノロジー	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
SupTech及びRegTech活用についての各国当局、規制対象機関へのサーベイ	SupTech及びRegTech	The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions	Financial Stability Board	2020年10月	【概要】 • SupTech、RegTechの拡大を供給側と需要側から説明。需要側は、規制の複雑化、効率性と有効性強化、支出の増大等、供給側は、利用可能性拡大、構造化・非構造化データ活用拡大、AI技術の向上、データアーキテクチュアの改善等。 • SupTechとRegTechのメリットは、監視、サーベイランス、分析能力を向上させ、データ収集と可視化を改善、リアルタイムでリスク指標を生成し、フォワードルッキングな判断に基づく監督や政策立案を可能とする点。規制対象機関にとっては、コンプライアンスのためのリスク管理能力を強化し、報告コスト削減。 • SupTechとRegTechのリスクと課題は、データ品質、サイバーリスク、コスト、風評リスク。特定の規制対象機関のシステム悪用可能性もある。民間部門とのデータサイエンティスト、エンジニアなどの人材獲得競争も起こりうる。 • データの収集、保存、管理、分析について、データの異質性、多様性、重複など多くの課題がある。非構造化データは有効であるが分析が困難である。データの増加は保存コストを増加させうる。データ分析可視化ツールとしてエクセルが使われるが、PythonやRを使う機関もある。自然言語処理（NLP）に基づくSupTechツールも使われている。 • SupTech や RegTech の活用において、コスト節減、データ向上のために規制当局と規制対象機関の協力、テクノロジーベンダーとの連携はより活発化している。規制対象機関による新技術の応用が進んでおり、AIや機械学習の技術が、不正検知、報告、リスク管理、AML/CFTなどに活用されている。規制対象機関のRegTechへの過度の依存は、過去のデータへの依存によるバイアスの存在やサイバーリスクなど問題を起こす可能性があり、規制当局、RegTechプロバイダー、規制対象機関の対話が必要である。	FSBが各国規制当局および規制対象機関に対して、SupTech及びRegTechの現状について問い合わせ、回答を得た広範なサーベイ。当局によるSupTech及び規制対象機関によるRegTechの活用は多くの機関により実施されており、また、内容は日進月歩。効率性と有効性、AIなどの技術の発展もあり、今後も一層活用されていくと考えられているが、技術人材の不足など懸念要素も多い。公的機関と民間、テクノロジープロバイダーの間で協調する必要がある。

出典：https://www.fsb.org/uploads/P091020.pdf

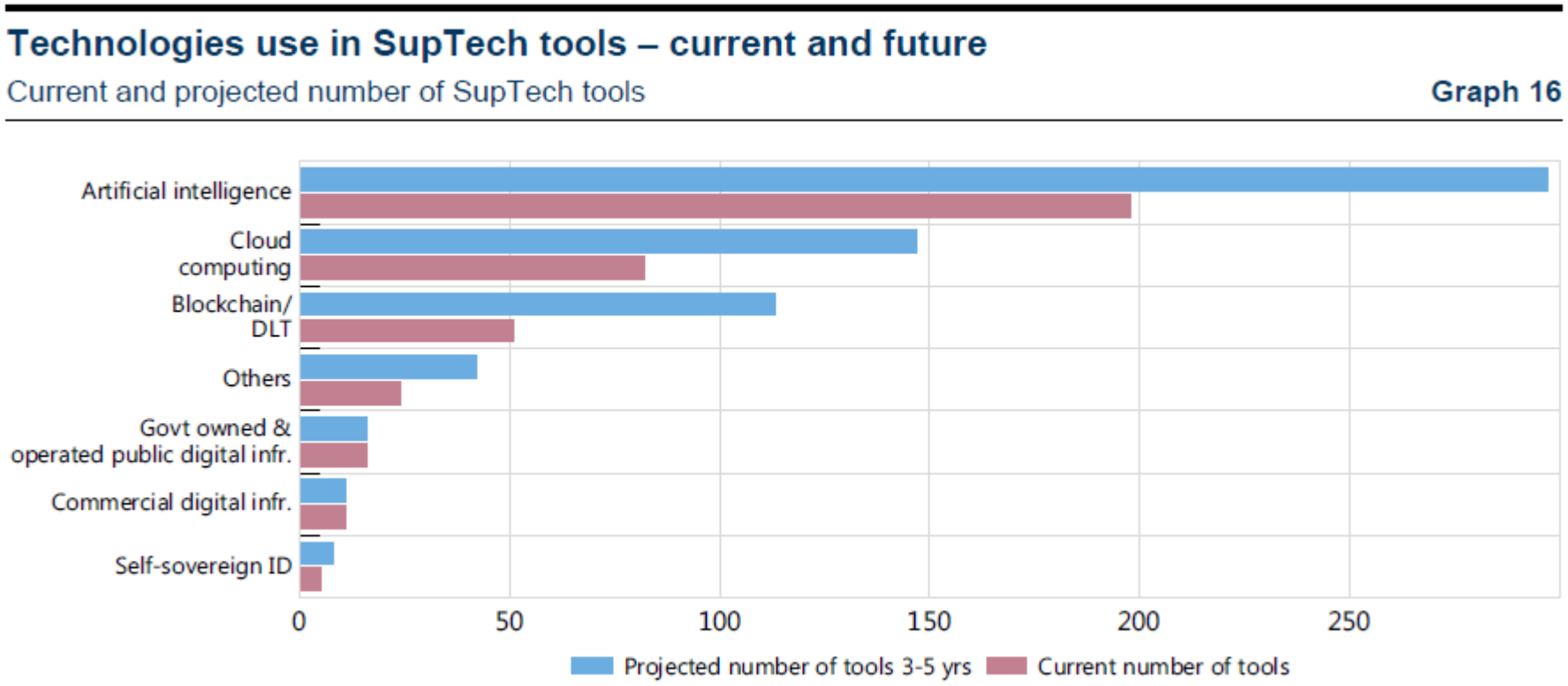
１　当局等が関与するRegTech/SupTechの検証プロジェクト

プロジェクト名	概要
SupTech及びRegTech活用についての各国当局、規制対象機関へのサーベイ	【プロジェクト参加者】 • アルゼンチン、オーストラリア、ブラジル、カナダ、中国、ECB、フランス、ドイツ、香港、インド、インドネシア、イタリア、日本、韓国、メキシコ、オランダ、ロシア、サウジアラビア、シンガポール、南アフリカ、スペイン、スイス、トルコ、イギリス、アメリカの金融当局、規制対象機関 • 各国機関による２８ケーススタディ 【研究結果】 • IIFの調査によると、RegTechのストレステストの適用における課題は金融の安定性への影響を最小化するために、強力なガバナンスと監視が必要であることを示している。 • 規制当局による今後の技術利用において、人間ベースの監督プロセスも重要である。 • ルールを機械可読形式に変換し、APIなどを通じて、規制対象機関の規制報告や、当局のプル型監視を可能にする。 • AIは金融活動に関するタイムリーな洞察を提供し、従来の人間分析よりも効率的にデータを分析できる可能性があるが、適切な監視なしでは透明性や説明可能性、データの偏りから新たなリスクを引き起こす恐れがある。規制におけるAI使用の倫理は慎重に理解し、公共の利益に調整されるべきであり、データの信頼性や偏り、所有権に関する懸念が生じる可能性がある。これらのリスクを管理するためには、透明性と公平性を保つガバナンスが重要である。 • クラウドベースのサービスは、当局間の効率的かつ効果的な情報共有を可能にし、規制当局間の協力関係の強化に有効である。第三者プロバイダーへの過度の依存も引き起こす可能性がある。 • 規制当局は、SupTechツールをイノベーションラボのようなリソースを通じて学び、情報交換を行うことができる。最近の例としては、BISイノベーションハブがある。当局間での協力に大きな意欲があり、監督当局間の協力が想定される。 • 今後の課題として、当局は、独自の目的に合致した、ユーザー中心の明確なSupTech戦略を必要としている。当局は、必要なデジタル・スキルセットを持つ必要な人材を惹きつけ、維持する必要がある。SupTech ツールの開発または取得の目標を戦略的に理解した専門家の採用が重要で、技術開発について遅れを取らないために、当局は、他の金融当局、学界、技術ベンダー、国際機関など、さまざまな外部関係者と関わりを持ち、革新的な協力関係を模索することを検討すべきである。さらに、適切な職員研修プログラムは、知識を向上させ、加速させるために重要である。 • 基準設定主体や当局は、報告ソリューションの拡張性や相互運用性を高めるため、国際協力の可能性を含め、関連する規制分野における共通のデータ標準や分類法を評価すべきである。 • 収集されるデータの量と豊富さが急速に増大する中、当局は、新たなテクノロジーの活用、高度な分析ツールの使用、適切なデータガバナンスの枠組みが必要となる。ツールの説明可能性と、ツールの利用結果がどのように意思決定に反映されるかについての透明性の確保、当局内の説明責任が重要である。 • SupTechとRegTechはまだ比較的新しい分野であるため、パイロットや概念実証が必ずしも最初から成功するわけではない。一方、当局や規制対象機関は、協調と革新の精神を奨励・育成し、当局は、将来の規制状況の基礎を築くオープンな対話と議論を奨励することができる。

プロジェクト名	概要
SupTech及びRegTech活用についての各国当局、規制対象機関へのサーベイ	• 本プロジェクトの会員を対象とした調査結果として、RegTechツールに用いられているテクノロジーについて、以下に抜粋した。 • RegTechツールを牽引する主要テクノロジーについて、は、ML、NLP、クラウドコンピューティングであり、ブロックチェーン技術の割合は相対的に低いことが示されている。 • ブロックチェーン技術が適用されている分野としては、KYC・身元確認・当人認証やリスク管理などとなっている。 図2-1-2　RegTechツールに用いられているテクノロジー 

プロジェクト名	概要
SupTech及びRegTech活用についての各国当局、規制対象機関へのサーベイ	• 今後の展望として、現在導入しているSupTechツールの数と、今後3～5年間に導入すると予想されるツールの内訳を本プロジェクトの会員に尋ねた結果のグラフを以下に抜粋した。AI、クラウドコンピューティング、ブロックチェーン/DLTアプリケーションは、今後最も導入される可能性の高いツールと判断されている。

図2-1-3　SupTechツールに用いられている、用いられるであろうテクノロジー



１　当局等が関与するRegTech/SupTechの検証プロジェクト

プロジェクト名	対象ブロックチェーン	文献名	作者	発行年月	プロジェクト概要	当研究に関連する記述など
DeFiに関するPublic consultation	DeFi イーサリウム	“Decentralised” or “disintermediated” finance (DeFi): what regulatory response?	Olivier Fliche, Julien Uri, Mathieu Vileyn FinTech-Innovation Hub Autorité de conrrôle prandentiel et de résolution（ACPR,健全性監督機構）	2023年９月	【概要】 • ACPRは、分散型金融（DeFi）のリスクを分類し、それに対応する規制案を提案するディスカッションペーパーを公開し、広範な意見募集を実施した。DeFiにおける集中化現象やレイヤー2ソリューションのリスク、スマートコントラクト認証の必要性など、幅広いテーマが議論され、パブリックチェーンの強化やスマートコントラクトの規制基準を中心に多様な視点が提示された。 【研究結果】 • パブリックチェーンの使用が支持された一方、スマートコントラクト認証の方法や範囲には意見の相違が見られた。 • レイヤー2ソリューションや分散型オラクルのリスクに関する多様な見解が示された。 • ステーブルコインにMiCA規則を適用する提案には賛否が分かれた。 • DeFiの本質的リスクである集中化に対して、「ガバナンス最小化」や公共機関による監査が提案された。また、利用者保護のためのアクセス規制の必要性が広く認識された。 【従来の研究との新規性】 DeFiの規制を検討するにあたり、パブリックチェーンの脆弱性に関する議論やスマートコントラクト認証の基準設定など、具体的な実務的提案が行われた。	本パブリックコンサルテーションの成果は、MICA規制についての欧州での議論について、ACPRよりのインプットとして使用される。DeFiのクライアント保護についてのガバナンス、オペレーションガイドラインを示すことで、さらなる活用の可能性を検討しようとするもの。業界関係者が多いため、活用については反対の声は非常に少なく、むしろ発展させ活用してゆこうという方向。 スマートコントラクト認証について、更なる検討を求めている。 参加者より様々な技術的提案がなされており、解決可能性のある問題もある一方、きわめて根本的な問題も散見されており、今後も研究と検討が必要となっている。

出典：https://acpr.banque-france.fr/en/decentralised-or-disintermediated-finance-defi-what-regulatory-response

プロジェクト名	概要
DeFiに関するPublic consultation	【研究内容】 • DeFiのリスク分析：分権ガバナンスに関するリスクは、ガバナンス・トークンの大半が寡占、独占されることにより、「偽りの分権化」のように見える。ガバナンスメカニズムの透明性が重要であるが、中央集権的な要素を完全に排除することは不可能。よって、「ガバナンスの最小化」という原則も一つの提案事項として検討しうる。これをスマートコントラクトの認証の基準の一つとすることも一案として提示している。 • DeFiの３層構造、ブロックチェーンインフラ、アプリケーション、ユーザーデバイスが区別され、高度に集中されたガバナンスについて述べられており、その特性に合わせた規制オプションの検討がなされている。 • DeFiのガバナンスは、収穫逓増の性質のため、独占・寡占状態にあり、ブロックチェーンノードをホストするインフラとクラウドプロバイダーの役割が重要と指摘した。 • プロトコル・ガバナンスに関するフラッシュローン攻撃のリスクについては、プロトコル上の保護メカニズムや提案の提出と投票のプロセスの透明化によってリスクを最小化できる可能性がある。 • 技術的な異質性に伴う多様な「レイヤー２」ソリューションのインフラリスクについては、ブロックチェーン接続ブリッジのセキュリティなどが存在する。拡張性の課題についてエコシステムの成熟を求めるべく、引き続き研究が必要としている。 • ブロックチェーンとプロトコルに対するコンピュータ攻撃のリスクについては、「サンドイッチ攻撃」などのリスクがあるが、レイヤー１のブロックチェーンのみならず、レイヤー２のソリューションに使用されるmempool（メモリプール）についての問題も指摘される。 • ほとんどのブロックチェーンにて使用されている仮名性に基づくAML/CFTリスクも指摘。逆に参加者のプライバシー保護要件との両立が難しいが、技術革新によりデジタルIDソリューションが開発されており、この問題を解決できる可能性がある。 • スマートコントラクトを認証するという原則は支持されたが、その方法はまだ検討中とした。 • 仲介業者やユーザーインターフェースに対する規制の枠組みの必要性を指摘している。 【制限事項】 DeFi技術の成熟度が低いため、提案された規制案の実効性や技術的妥当性については継続的な検討が必要とされる。 【応用可能性】 欧州MiCA規則の枠組みを補完する形で、DeFi規制案が金融安定性の向上や利用者保護に寄与する可能性がある。

２　分散型金融におけるRegTech

1章でとりあげた事例（Fireblocks,Uniswap,Circle,Verite）に関して、分散型金融システムの取引主体によって利用されうる、規制・報告義務等の法令遵守をサポートするイノベーティブな技術であるRegTechに相当する機能を以下の表に示す。また、それらに関連して、IOSCOの“同じ活動、同じリスク、同じ規制・規制結果 ”という指導原則に照らし、ブロックチェーン技術を用いている分散型金融と規制要件を満たした伝統的金融のRegTechに相当する機能を対比して紹介することで、分散型金融におけるRegTechの意義を考察する。※ここで紹介しているRegTech関連機能は、被規制機関が監督対応として求められたときに効率的に対応するための機能の実装状況であり、これらが各国の規制要件を満たした効果があるかの検証は別途必要である点に留意。なお、効率的に監督できるかどうかはSupTechの観点からの検証であり、3章に記載する。

分散型金融システム	規制機能	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Fireblocks	取引モニタリング	すべてのトランザクションに対して、リアルタイムのトランザクション スクリーニング、リスク スコアリング、およびコンプライアンス アクションを有効にできる。リスクのあるウォレットへの送金、リスクあるウォレットからの受信トランザクションのどちらも凍結可能。 事前に定義されたルールに従って取引を評価し、リアルタイムでモニタリングされる（凍結は手動）。疑わしい取引の検証判断と当局への必要情報報告の全てをルール判断で完結しえないが、ブロックチェーン技術の特性であるトレーサビリティにより、効率性向上が期待される。	伝統的金融機関は、中央集権的なシステムを利用して取引のモニタリングを行う。取引モニタリングは、主に自動化されたツール（ルールベースのシステムや機械学習アルゴリズム）を使用して行われる。取引はリアルタイムでモニタリングされる場合もあれば、一定の期間の過去取引と顧客属性・リスク評価データを用いてモニタリングされる場合もある。 これには、自動化が困難な顧客へのヒアリングや資料提出依頼（面談や電話）などの人を介する調査が含まれる。	Fireblocksを利用する分散型金融システムの運営責任者	AML/CFT/CPF
	アカウントのスクリーニング	アドレス スクリーニングを自動化して、潜在的にリスクのあるウォレットをプラットフォームとやり取りする前に特定する。取引履歴やウォレットアクティビティといったオンチェーンデータをスクリーニングに用いている。 ブロックチェーン技術の特性であるトレーサビリティにより、効率性向上が期待される。	伝統的金融機関は、システムを利用してアカウントのスクリーニングを行う。アカウントのスクリーニングは、主に自動化されたツール（ルールベースのシステムや機械学習アルゴリズム）を使用して行われ、最終判断はコンプライアンス責任者に委ねられるなど人を介する。 これには、自動化が困難な顧客へのヒアリングや資料提出依頼（面談や電話）による人を介する調査が含まれる。		

出典：Fireblocks「Compliance Integrations」https://www.fireblocks.com/platforms/compliance/

２　分散型金融におけるRegTech

分散型金融システム	規制機能	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Fireblocks	トラベルルール	暗号資産サービスプロバイダー (以下、VASP)からの転送に関するトラベルルールレポートを自動的に生成し、法域区域全体で他のプロバイダーからのリクエストを検証する。 • VASP 向けのエンドツーエンドのトラベルルール • データ転送リクエストを承認および拒否 • 基準を満たすトランザクションを自動化 • ビジネス パートナーの自動識別および検証 • 顧客情報を安全に交換および保存 • トラベルルールに関するレポート生成 トラベルルールの補足説明： FATFが各法域に「トラベルルール」の導入を要請しており、我が国では「暗号資産・電子決済手段の取引経路を追跡することを可能にするため、暗号資産交換業者・電子決済手段等取引業者に対し、暗号資産・電子決済手段の移転時に送付人・受取人の情報を通知する義務」（犯罪による収益の移転防止に関する法律　第十条の三、第十条の五）と定義している。 VASPがデジタル資産を取引する場合、特定の顧客データを収集して通知することが義務付けられているが、現在、各法域では通知要件と施行時期が異なり、施行方法が異なる。企業は、法域全体でトラベル ルール要件を管理して遵守し、自社とその取引先のコンプライアンスを確保できるソリューションを必要としている。	FATFから、「勧告16：電信送金（海外送金）」にて、以下が示されている。 「各国は、金融機関が、正確な必須送金人情報、及び必須受取人情報を電信送金及び関連する通知文（related message）に含めること、また、当該情報が一連の送金プロセスを通じて電信送金、又は関連電文メッセージに付記されることを確保しなければならない。」 また、“「暗号資産・暗号資産交換業者に関する新たなFATF基準についての12ヵ月レビュー」におけるトラベルルールの課題- 暗号資産移転と銀行送金を比較して“にて、以下が示されている（抜粋）。 この要件は、一般的に金融機関が支払指図をSWIFTや決済システムへ発信する際、必要情報を正確に含めることで履行されている。（中略）たとえ受取人の銀行口座番号を知っていても、その口座が「どこにあるか」を知らなければ振込む術はない。この共通認識が定着しており、送金を受けたい場合、先方には銀行名（場合によっては、銀行の所在国・支店名あるいは支店番号）と口座名義を口座番号と共に伝えるだろう。SWIFTコード等で受取金融機関や事業法人を指定することもあるが、その場合でも、中央管理者が公表するコード一覧さえ見れば、どの銀行・事業会社か判別できる。これに対し、暗号資産のウォレットアドレスでは、そのようなリストはない。暗号資産の種別・送付・受取ごとにアドレスが異なるのみならず、都度変更もあり得る。	Fireblocksを利用する分散型金融システムの運営責任者	AML/CFT/CPF

出典： https://www.fsa.go.jp/frtc/kikou/2020/FSA_article_ACAMSToday2020_Sept-Nov.pdf

２　分散型金融におけるRegTech

分散型金融システム	規制機能	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Fireblocks	トラベルルール	上記に関しては、Fireblocksが認証（VASPの所在国・金融監督当局・登録・免許有無等）したVASPリストに依拠する包括的な対応が可能なシステムといえる。 伝統的金融機能と同等を目指すものといえるため、分散型金融のRegTech機能に特段の優位性は認められないと考えられる。	－	－	－
	KYC	DeFi流動性市場である Aave Arc の Fireblocks Permissioned DeFiでは、参加者承認手続きを得て、KYC に合格することで、Fireblocks のホワイトリストに登録される。これにより、Aave Arc 内で入金、借り入れ、清算が可能となる。 上記に関しては、Fireblocksが認証した参加者リストに依拠する中央集権的なシステムといえる。 現状は伝統的金融機能と同等を目指すものといえるため、分散型金融のRegTech機能に特段の優位性は認められないと考えられるが、将来的にブロックチェーン関連技術を用いることで、金融機関同士で安全にKYCデータ共有が可能となれば、金融セクター共有の課題である、KYCオペレーションの重複コスト問題の削減が期待できる。 さらに、ゼロ知識証明などの暗号技術を用いることで、KYCに必要な情報を提供しつつ、顧客の個人情報を保護することが可能になる。これにより、顧客はプライバシーを犠牲にすることなく、KYC手続きを完了することができる。	伝統的金融におけるKYCプロセスのRegTech関連機能は次のとおり。 ・顧客が本人確認のため、提示した身分証明書や住所証明書などの情報をスキャンし、自動的に読み取り、真贋を分析する ・（既存）顧客の職業などの属性、取引履歴や金融状況などを分析し、マネー・ローンダリングやテロ資金供与のリスクを自動的に評価する ・顧客が制裁対象者リストに掲載されていないことを自動的に確認する（口座開設時、制裁対象者リスト更新時） KYCの補足説明： KYCの方式として、対面式、郵送、オンラインの3種類があるが、我が国のオンライン方式では、犯収法上の分類であるところの「ホ）自撮り撮影と写真付本人確認書類」「ヘ）自撮り撮影と写真付本人確認書類のIC情報」「ト）写真付本人確認書類の撮影、IC情報、銀行照会あるいは銀行口座に少額送金」「ワ）マイナンバーカードの公的個人認証サービスの電子署名」などが使われている。	Fireblocksを利用する分散型金融システムの運営責任者	AML/CFT/CPF

分散型金融システム	規制機能	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Uniswap	取引審査、アカウントのスクリーニング	Fireblocksと同様の機能を提供していると考えられる。	Fireblocksの記載を参照	UniswapのDAO（責任の主体者が特定しにくい）	AML/CFT/CPF
	KYC	FireblocksやVeriteなど、外部のKYCソリューションとの連携機能を提供している。 ※本文書では、Fireblocksなども含む外部のKYCソリューション全般として、どの法域のKYC要件を満たすのか未確認である点に留意。	Fireblocks、Veriteの記載参照		

分散型金融システム	規制機能	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Circle	残高確認	USDC の埋蔵量は、関連するミント/バーンとともに毎週、開示されている。四大会計事務所は、USDC 準備金の価値が流通している USDC の額より大きいという第三者保証を毎月提供している。 報告書は、米国公認会計士協会 (AICPA) が定めた証明基準に従って作成されている。 USDCの埋蔵量（ミントとバーンのネット）の残高確認手続きははオンチェーン上の公開情報であるため、Circleによる開示情報に対する監督確認手続きは透明性（客観性）と即時性といった特性がある。 なお、ウォレットアドレス単位の残高確認については、オンチェーンデータを閲覧できるツールがあり、これも透明性（客観性）と即時性といった特性があるといえる。	ここでは、銀行の残高確認手続におけるRegTechソリューションとして、会計監査確認センター合同会社によるBalance Gatewayというサービスを例に紹介する。 ・複数の確認状（債権債務残高、銀行等取引残高、証券取引残高、弁護士確認など）に対応 ・オンラインで確認できる（以下の手順はすべてWeb上の手続き） 1.被監査会社または会計監査人による回答依頼の作成 2.被監査会社による回答依頼の承認 3.会計監査人による回答の依頼 4.回答者による回答の入力 5.会計監査人による回答の確認 Balance Gatewayは、監査法人トーマツのサービスであり、他の監査法人は利用できない点やすべての金融機関に対応しているわけではない点に留意。	Circle	利用者保護／会計監査における確認の書面(残高確認状、残確、などという)による回答は義務化されていない（法的根拠はない）。

出典：Circle「Transparency & Stability」 https://www.circle.com/en/transparency
会計監査確認センター合同会社「Balance Gatewayとは 」https://auditconfirmation.co.jp/bg.html

２　分散型金融におけるRegTech

分散型金融システム	分散型金融のRegTech関連機能	伝統的金融のRegTech関連機能	監督対応データの提供者	規制・報告義務等の関連法令
Circle(Verite)	Veriteは、Circleが提唱する分散型の認証および身元確認のプロトコルであり、ブロックチェーン上での信頼性の高いID確認を実現することを目的としている。 Veriteを利用することで、ユーザーは自分のID情報を管理し、信頼できる形で分散型金融システムなどのサービス提供者に提示できるようになるという。 VeriteのRegTech上の目的は、以下の通り。 KYCおよびAMLの効率化： 金融機関やサービス提供者がKYC/AML規制をより効果的に遵守することを目的としたユーザーのID確認プロセスの自動化 データのプライバシーとセキュリティの強化： Veriteプロトコルは、ユーザーの個人情報を分散型ネットワーク上で安全に管理することを目的としたデータのプライバシー保護 規制遵守の透明性向上： ブロックチェーン技術を活用することによる取引やデータ管理の透明性の向上 現状は伝統的金融機能と同等を目指すものといえるため、分散型金融のRegTech機能に特段の優位性は認められないと考えられるが、将来的にブロックチェーン関連技術を用いることで、金融機関同士で安全にKYCデータ共有が可能となれば、金融セクター共有の課題である、KYCオペレーションの重複コスト問題の削減が期待できる。	Fireblocksの記載を参照	Veriteを利用する分散型金融システム	AML/CFT/CPF

第２章 ブロックチェーン技術等のRegTech/SupTechへの活用可能性
３　総括

２章１では、「当局等が関与するRegTech/SupTechの検証プロジェクト」として、RegTechやSupTechの可能性に関する当局等の見解などを紹介した。なかでも、被規制金融機関あるいは当局等が埋め込み型監督や監督ノードを用いることで、トークン取引状況を効率的に監督できる可能性が言及されていた。

２章２では、「分散型金融におけるRegTech」として、1章でとりあげた事例（Fireblocks,Uniswap,Circle,Verite）に関して、分散型金融システムの取引主体によって利用されうる、規制・報告義務等の法令遵守をサポートするイノベーティブな技術であるRegTechに相当する機能を紹介した。また、それらに関連して、IOSCOの“同じ活動、同じリスク、同じ規制・規制結果 ”という指導原則に照らし、ブロックチェーン技術を用いている分散型金融と規制要件を満たした伝統的金融のRegTechに相当する機能を対比して紹介することで、分散型金融におけるRegTechの意義を考察した。

そこで、第３章では、既にトークン（暗号資産）取引を活発に行っている暗号資産交換業者に関するRegTechおよびSupTechの技術的な可能性と課題を検証していく。

第３章　ブロックチェーンの特性を活用したRegtech/Suptech等に関する机上検証

第３章　ブロックチェーンの特性を活用したRegtech/Suptech等に関する机上検証

第３章に登場する主な専門用語について、以下のとおり定義する。

用語	定義
デプロイ（deploy）	Webアプリケーションなどのシステム開発工程で、アプリケーションの機能やサービスをサーバー上に配置・展開し、利用可能な状態にする一連の作業を指す。 デプロイはテスト環境と本番環境を利用して、サーバー上に実行ファイルを反映し、実際に稼働できる状態にする。
バリデータ	一般に、ブロックチェーンネットワークにおいて、取引の検証とブロック生成を行う役割を担うノードのことを指す。
オフチェーンデータ	ブロックチェーン上に記録されていないデータを指す。多くは企業内のデータベースや、紙媒体の書類などで管理されている。

第３章　ブロックチェーンの特性を活用したRegtech/Suptech等に関する机上検証
１　監督シナリオの考慮要素

第３章では、暗号資産交換業者に対する監督シナリオに基づいて、RegTechおよびSupTechの技術的な可能性あるいは制約条件を検証する。

被規制金融機関が取り扱うトークン取引の性質としては、第1章７で整理した「表1-7-1　被規制金融機関が取り扱うトークン取引の性質」を踏襲し、以下のパターンについて、検証する。

取引シナリオ	説明
暗号資産交換業者による暗号資産の取引	具体的には、暗号資産交換業者と外部の相互のウォレット間における暗号資産取引を想定している。 暗号資産交換業者内における顧客の暗号資産を保護預かりにした状態で、顧客同士が売買取引するオフチェーン上のケースについてはシナリオに含めない。

本机上検証は、FSB等の国際機関による報告書で言及されているトークナイゼーションや分散型金融に関連するリスクや脆弱性を踏まえ、簡素なシナリオを想定し、埋め込み型監督・監督ノードによるリスク低減効果を検証することを目的としている。特に、当局による対応（Suptech）においては、当局が自ら監督ノードを構築しデータ分析等を行うシナリオを想定している。なお、本検証はRegtech/Suptechの可能性を検証するために、大胆な仮説を置き限定的な範囲で実施したものであり、我が国の規制要件への準拠等を十分に考慮したものではないことに留意すること。

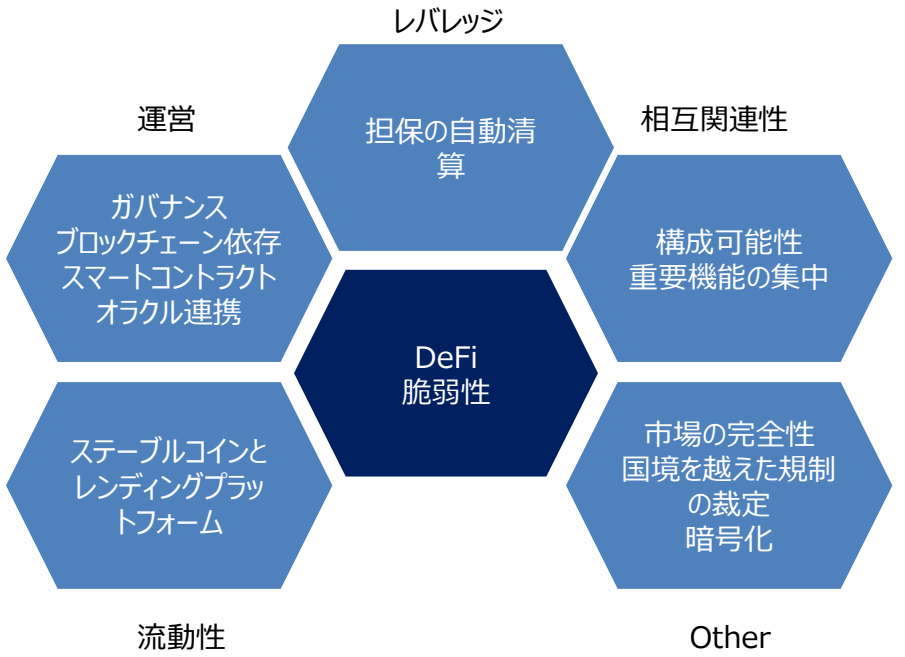
１　監督シナリオの考慮要素

FSBの報告書によれば、多機能暗号資産仲介機関（以下、MCI）の金融安定におけるリスクと脆弱性を表3-1-1、DeFiの特徴と脆弱性を図3-1-1としている。本文書における暗号資産関連の監督シナリオは、これらのリスクや脆弱性を参考に作成する。

表3-1-1　MCIの金融安定におけるリスクと脆弱性

リスクと脆弱性
顧客資金の横領
詐欺
自己の投資トークンに対する投機的活動や、透明性のない供給管理活動を通じた市場操作
価格操作／ボラティリティ
ウォッシュトレーディング
フロントランニング
顧客に対して不利な取引、あるいは顧客より有利な取引
利益相反
過度のレバレッジ（例：担保として自らの投資トークンを再利用する）
流動性
信用リスク
供給と準備のミスマッチ（適切な保護措置のない準備金の不正流用や端数準備など）
相互接続 - 反競争的慣行による集中リスクの悪化
相互接続 - 相互依存（例：オラクル）
技術的および運用上の脆弱性

図3-1-1　DeFiの特徴と脆弱性のまとめ



出典　FSBの報告書「分散型金融の金融安定化リスク

表3-1-1　FSBの報告書「多機能暗号資産仲介機関の金融安定性への影響」の付録1：MCIにおける機能の組み合わせに関連するリスクと脆弱性から、クニエが加工して作成した

２　RegTechとSupTechにおける監督シナリオ

取引シナリオに対し、用意した監督シナリオは次のとおり。

表3-2-1　RegTechとSupTechにおける監督シナリオ

要件種別	RegTech（埋め込み型監督）	SupTech（監督ノード）
取引モニタリング	①　トークン取引が成立する前に、認証済ウォレットであることを確認する仕組み。認証済みウォレットでないと判断した場合は取引処理を実行しない。 ここでいう認証済みウォレットとは、VC/DID提供者による認証や、暗号資産交換業者（およびそのKYC済み顧客）から暗号資産移転であると確認できるウォレットの想定。	左記報告内容について、当局がブロックチェーン上に用意したノードで得られるデータをもとに検証する。
	②　トークン取引データを対象に、あらかじめ定義した疑わしい取引パターンに該当する取引を抽出し、顧客のKYCや属性など、追加情報を追加の上、所定の当局に報告する。疑わしい取引の届け出義務に則った報告を念頭におくもの。	
レポーティング	当局からの報告徴求（定期・都度）に応じられるよう、トークンに関する各種データを保存し、当局に報告する。	左記報告内容について、当局がブロックチェーン上に用意したノードで得られるデータをもとに検証する。

３　監督シナリオが求めるシステム機能

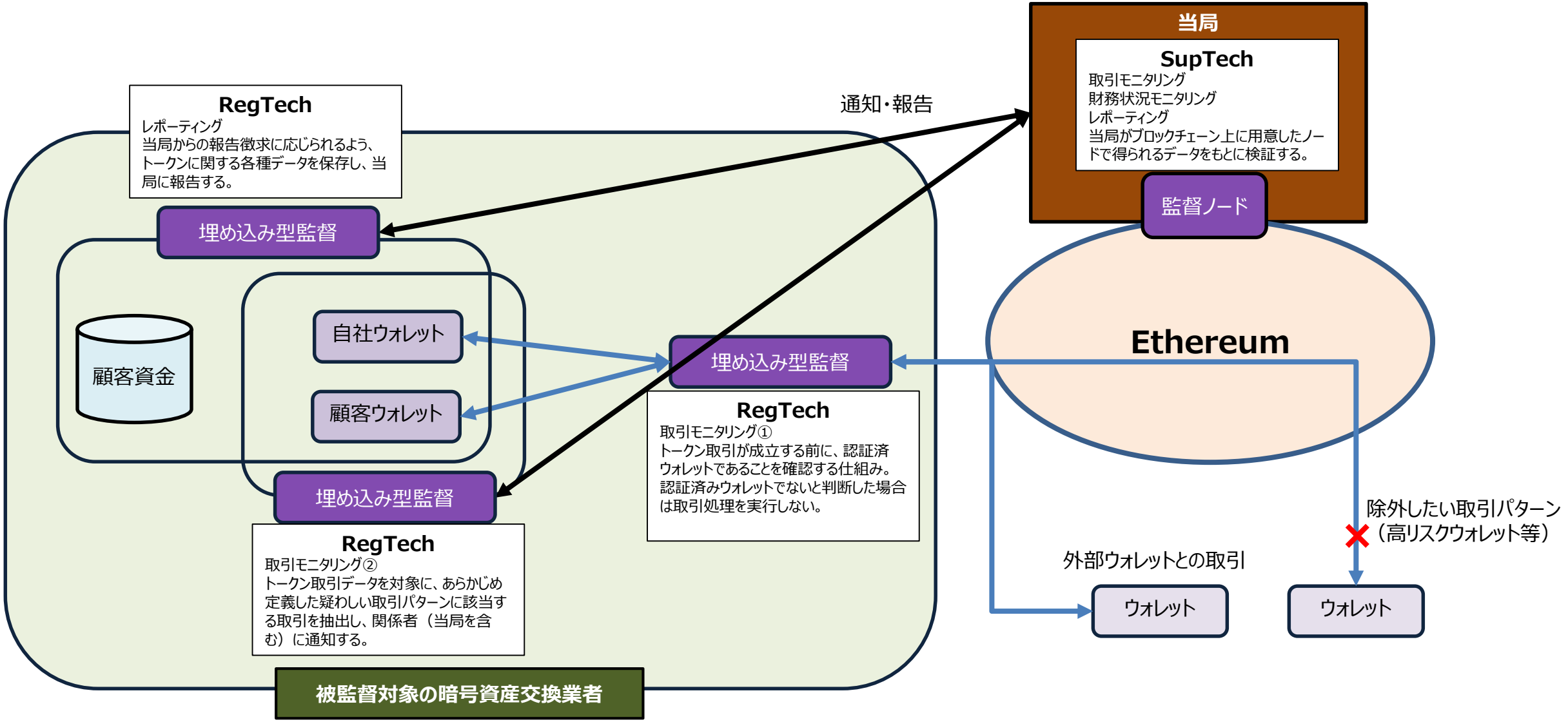
以下に要件種別ごとのシナリオに対して求められる主なシステム機能を示す。

表3-3-1　監督シナリオが求めるシステム機能

要件種別	RegTech/SupTech	主なシステム機能
取引モニタリング	RegTech	金融取引データのリアルタイムモニタリング 不適切な金融取引の検知 特定のルールにおける金融取引の制御（特定取引を停止） 取引参加者のKYC
	SupTech	金融取引データの検証 規制機関による監視活動やデータ分析の過程を外部から見えないようにする
レポーティング	RegTech	取引モニタリングおよび財務状況モニタリングの内容報告
	SupTech	取引モニタリングおよび財務状況モニタリングの内容検証

４　取引シナリオのシステム構成

各監督シナリオについて、システム構成（パーミッションレスチェーン：Ethreum）を以下に示す。



取引シナリオ：暗号資産交換業者による暗号資産の取引

埋め込み型監督および監督ノードが有効に機能しうるか検証する。

監督シナリオ	システム要件	検証内容	RegTech（埋め込み型監督）における有効性検証
			イーサリアム
RegTech 取引モニタリング	金融取引データのリアルタイムモニタリング	リアルタイムの異常値検出が可能か	埋め込み型監督によって、オンチェーン上のデータをモニタリングすることができるため、リアルタイムの異常値検出が可能といえる。
	不適切な金融取引の検知	どのような異常値検出が可能か	埋め込み型監督によって、オンチェーン上のデータ（ブロック番号、送信元アドレス、送信先アドレス取引数量、トークン種別、トランザクション手数料、タイムスタンプ）をモニタリングすることで、疑わしい取引のアドレス、数量の取引を自動的に検出することができる。
	取引のルールにおける金融取引の制御（特定取引を停止）	暗号資産交換業者から外部の暗号資産アドレスに対して、暗号資産が転送された後に、取引を停止できるか	イーサリアムでは、例えばドラフトであるが ERC-1644 がセキュリティトークンの強制転送を定義し、組戻し等に用いることが可能となっており、スマートコントラクトの構成次第で取引停止機能の実装の余地がある。
	取引相手のKYC	送金元、送金先のKYC状況を確認できるか	アドレス（公開鍵から生成される）だけでは本人かどうかを証明できない。前提として、国内の暗号資産交換業者同士であれば、KYC済みの顧客属性とアドレスを紐づけて管理しているため、送金元、送金先のKYC状況は確認できる。他方、海外の暗号資産交換業者にはKYC済みではないケースや、個人が生成したウォレットアドレスなど、KYC状況が確認できないことがある。
RegTech レポーティング	取引モニタリングの内容報告	網羅性があり、追跡可能な内容を報告できるか	適切な取引モニタリングおよび財務状況モニタリングが実施されていれば、網羅性や追跡可能性が有効な報告が期待できる。

５　システム要件における検証項目と検証結果

監督シナリオ	システム要件	検証内容	SupTech（監督ノード）における有効性検証 イーサリアム
SupTech 取引モニタリング	金融取引データの検証	疑わしい取引があった場合などに金融機関から提示されるデータが正当なものかどうか確認ができるか、また、その方法はどのような手段がありえるか	当局自らノードを構築することで、外部のサービスやプロバイダーに依存せずにEthereumネットワークにアクセスできるという点で、自己依存性が高まる。例えば、Etherscanがダウンしたり、制限を設けたりしても、影響を受けることはない。 しかし、運用する場合は、要件上ブロック検証に参加する必要はないものの、ネットワークの全履歴にアクセスできる必要があることからアーカイブノードの運用が前提になると考えられる。 アーカイブノードを運用する場合、ネットワークの全履歴にアクセスできるようになる一方、データ容量が非常に大きくなる。これは技術的には可能であるが、運用には、定期的なメンテナンスにかかる人件費に加えて、サーバー費等のコストが発生する。具体的には、アーカイブノードの運用に必要なストレージ容量は、2023年10月時点で約12TBと推定され、さらに年々増加している。この規模のデータを保存・運用するためのサーバー費用は、クラウドサービスを利用した場合、月額数十万円程度になると予想される。さらに、ハードウェアの保守やソフトウェアのアップデート、セキュリティ対策など、継続的なメンテナンスに人件費が発生する。これらのコストを考慮すると、費用対効果の面からサードパーティーのサービスを利用することが現実的である可能性もある。
	活動の秘匿	当局が取引モニタリングを行っていることが外部に公開されず秘匿性を維持できるか	監督ノードの存在は第三者に秘匿できないが、監督ノードであるかどうかは判断できず、モニタリングしている内容について秘匿が可能。
SupTech レポーティング	取引モニタリングの内容検証	第三者に報告内容を秘匿できるか	自らノードを運用する場合は、データ容量が非常に大きくなり、定期的なメンテナンスにかかる人件費に加えて、サーバー費等のコスト面で実現可能性は低いと考えられる。

出典：https://ethereum.org/ja/developers/docs/nodes-and-clients/archive-nodes/

第３章　ブロックチェーンの特性を活用したRegtech/Suptech等に関する机上検証
6　総括

伝統的金融機関におけるトークナイゼーションにおいて、被規制金融機関及び当局等による埋め込み型監督および監督ノードがRegTech/SupTechとして活用可能か、について机上検討した結果を以下に総括する。

３章１では、「監督シナリオの考慮要素」として、金融安定におけるリスクと脆弱性やDeFiの特徴と脆弱性をあげた。

３章２では、「RegTechとSupTechにおける監督シナリオ」として、3章１の考慮要素をふまえた監督シナリオを示した。

３章３では、「監督シナリオが求めるシステム機能」として、埋め込み型監督および監督ノードのシステム機能を示した。

３章４では、「取引シナリオのシステム構成」として、各取引シナリオにおける埋め込み型監督および監督ノードの構成を図に示した。

３章５では、「システム要件における検証項目と検証結果」として、RegTechあるいはSupTechとして、埋め込み型監督および監督ノードに有効性があるかどうかの検証した。

SBI金融経済研究所のレポートにおいて、「パブリックチェーン上での取引は、流出事故への対応が困難となることや、AML/CFTリスクが高まることが想定される。秘密鍵を管理するウォレットを個人投資家が管理する想定とすれば、リスクは相応に残ることとなる。（中略）AML／CFTのリスク低減や、金利・配当支払いや売買差益等の税捕捉についてはKYCが重要となることから、規制金融機関によるKYCに依拠することになる。（中略）ホワイトリスト化されたウォレットのみが取引可能とするなどの手当てが必要になるものと思われる。」との指摘がなされている。

FSBの報告書によれば、SupTechに導入すると予想されるツールとして、AI、クラウドコンピューティングに次いでブロックチェーン/DLTアプリケーションが挙げられていた（本文書　P.61参照）。本報告書ではブロックチェーン技術（DLT)の発露として、埋め込み型監督および監督ノードの有効性を検証した。本文書で有効性が特に認められたシナリオは、パーミッションレスチェーンを用いた取引を行う暗号資産交換業者による埋め込み型監督とパーミッションドチェーンを用いた取引を行う伝統的金融機関に対する当局運営想定の監督ノードであった。また、FSB報告書では、ブロックチェーン技術を用いたRegTechとして活用される分野として、KYC検証やリスク管理などの分野が示されていた（本文書　P.60参照）　。

本報告書では、埋め込み型監督および監督ノードがFSB報告書が示す分野の一部において、RegTech/SupTechとして活用されうることが示された。但し、検討結果が示すとおり、制約条件があることから、実装に際してはさらなる検討が必要となる。
本文書が、埋め込み型監督や監督ノードの有効性条件の参考となり、さらなる運用上、制度上の検討が進む機会を提供できれば幸いである。

出典：セキュリティトークン最新事情と将来展望：2024年夏　https://sbiferi.co.jp/report/20240725_1.html