2025 年７月 18 日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ４
「新たなテクノロジーとＣＢＤＣ」
第９回会合の議事概要

１．開催要領

（日時）2025 年３月 25 日（火）14 時 00 分～16 時 30 分
（形式）Ｗｅｂ会議形式
（参加者）別紙のとおり

２．プレゼンテーションとディスカッション

- 三井住友信託銀行株式会社より、「アセットトークナイゼーションの海外動向」に関するプレゼンテーションが行われた。プレゼンテーションのポイントは以下のとおり[1]。

  ・ 昨年、Ethereum 上で発行されたＢＵＩＤＬ（BlackRock USD Institutional Digital Liquidity）は、米国の法律に基づき、米大手運用会社 BlackRock が運用するＭＭＦ（Money Market Fund）を、米 Securitize 社が提供・管理するプラットフォーム上でトークン化し販売しているもの。主な機能としてステーブルコインＵＳＤＣへの即時換金や月次の分配金支払いを提供。現在では複数のパブリックブロックチェーンで購入可能となっている。

  ・ ＢＵＩＤＬの最大の保有者である Ondo Finance 社は、ＢＵＩＤＬを担保にＯＵＳＧ（Ondo Short-Term US Government Treasuries）トークンを発行し、さらに、ＯＵＳＧトークンはＤｅＦｉ（分散型金融）利用時の担保として活用されて他のステーブルコインや暗号資産が取引されている。このように、ＢＵＩＤＬの事例は、伝統金融の流動性がＤｅＦｉへ持ち込まれている点で興味深い。

  ・ ＢＵＩＤＬが提供する機能は、パーミッションレスブロックチェーン上のスマートコントラクトで実装されているため、コードの閲覧は基本的

[1] 詳細は以下のプレゼンテーション資料を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo250718b.pdf

にだれでも可能であるものの、本当に正しく実装されているかの検証は専門知識がなければ難しい。例えばＣＢＤＣのように一般的なユーザーを対象とするデジタル資産の設計を検討していく場合には、想定するユーザーがより安心して活用できる環境を整備していく必要性も示唆される。

・ 昨年末に報告書が公表されたＲＳＮ（Regulated Settlement Network）は、複数の米国大手金融機関が、ＳＩＦＭＡ（米国証券業金融市場協会）、Ｓｗｉｆｔらと共同で取り組んだ実証実験で、パーミッショントブロックチェーン上でのＤＶＰ決済や異なるネットワークとの相互運用性が検証された。同プロジェクトでは、Digital Asset 社が開発したブロックチェーン Canton Network が採用されており、同技術は独自プログラミング言語 DAML を用いることで関係者の閲覧権限コントロールを容易にし、伝統金融の取引において重要な高いプライバシー要件を実現している点が特徴。

・ プライバシー関連では、J. P. Morgan 社によるファンドのトークン化を事例にＰＥＴ（Privacy-Enhancing Technologies）を検証したレポートや、英中銀とＭＩＴによるゼロ知識証明関連技術などの技術の検証をした共同レポートが昨年公表されている。

・ 金融規制の順守やプライバシー管理を目的としたトークン規格として、ERC-3643（パーミッショントトークン）や LF Decentralized Trust 傘下のＯＳＳプロジェクトの Paladin で開発が進む Zeto トークンなどがある。

・ Web で取得したデータを第三者へ正当なものであると証明する Web Proof として、ＴＬＳ通信とゼロ知識証明関連技術を組み合わせた zkTLS が注目されている。ユースケースとして、例えばプラットフォーム間でのデータ移動時の正当性保証などが考えられる。

● 三井住友信託銀行株式会社のプレゼンテーションを踏まえ、参加者によるディスカッションが行われた。議論の概要は、以下のとおり。

（参加者）ＢＵＩＤＬは、パブリックブロックチェーン上で発行・流通するトークンであるが、ＡＭＬ／ＣＦＴの観点で問題はないのか。

（プレゼンタ）ＫＹＣ等の米国基準のオンボーディングが完了したユーザーのみ Securitize Markets にアクセスしＢＵＩＤＬの保有が可能となる設計と

なっており、パブリックブロックチェーン上であっても、Securitize 社の管理のもとで取引が進められる仕組みとなっている。

（参加者）米国債を直接トークン化した場合と比較した際の、ＭＭＦのトークン化であるＢＵＩＤＬの良さとは何か。なお、元本割れといったＭＭＦ固有のリスクはトークン化によって変わらないという認識でよいか。

（プレゼンタ）満期償還がある単一の米国債に比べて、継続して保有でき、価格安定化の運用オペレーションがなされるＭＭＦの方が、ＤｅＦｉに流通するトークンの裏付け資産として好ましいとして選ぶニーズがあるのかもしれない。ご認識のとおり、ＭＭＦ固有のリスクはトークン化によっては変わらず、元本割れは金融環境次第で起こり得る。現在のＤｅＦｉの規模は、伝統金融と比べると小さいため、ＤｅＦｉで何かショックが起こり仮にトークン化されたＭＭＦの投げ売りが起こったとしても、伝統金融への影響は限定的ながら、今後そういった波及経路のインパクトは、ＤｅＦｉの成長動向とともに注意が必要と考える。

（参加者）今回ご紹介頂いたような、利息分配等の投資家への還元や即時換金等の利便性の高いトークンが、今後幅広く使われるようになるのだろうか。またＣＢＤＣやトークン化預金に対する潜在的なニーズは、こうした動きに影響を受けるだろうか。

（プレゼンタ）利便性を高めるために自由に設計できるトークンは好まれていくと思われるが、利用者にとっては、トークンの価値を保証する主体が誰なのかは引き続き重要なポイントだろう。また、危機時の社会インフラとしての役割など、求められる機能や責任によっても利用者が選ぶサービスは変わってくる理解。

（参加者）伝統金融とＤｅＦｉの往来に関しては、以前から注目されていた分野ではあるものの、今回プレゼン頂いたトークン化の事例拡大に伴い、当局サイドからの関心が今後より高まってくるのではないか。各領域の境界が曖昧になり、相互に影響しあう可能性を踏まえると、マクロ的な金融安定の観点から考慮すべき事項や対応負担は増えていくと考えるが、そうしたコストに見合うだけのＤｅＦｉのメリットはどのように考えればよいだろうか。例えば、プログラマビリティやコンポーザビリティといったＤｅＦｉの技術的特徴が、実社会のフリクションを減らす側面はその一つかもしれない。

（プレゼンタ）例えば、黎明期のインターネットが、今のような状態になると誰も予測していなかったように、将来的にＤｅＦｉが、インターネットのように生活を便利にするインフラとして、今は想定していないメリットを提供する可能性もあると考える。金融の文脈においても、もともとは対面を前提とした取引で、それがある種のトラストを生み出していたころから、インターネットを通じたオンライン取引が当たり前となったように、ブロックチェーンを通じた取引も当たり前となる世界もあり得るのかもしれない。また、パーミッションレスブロックチェーン上であっても、価値の源泉であるトラストを必要とするニーズに対しては、トークンの規格として規制に準拠する機能を技術的に埋め込むことで、パーミションドの伝統金融と、パーミッションレスのＤｅＦｉが交わっていく世界もあり得るのかもしれない。

（参加者）Web Proof に関して強い関心がある。同技術を用いてどのような実験をされたのか。

（プレゼンタ）社外資格試験の合格報告にオンラインの試験サイト（マイページ等）を閲覧した情報を、zkTLS を利用して社内連携できれば簡単・迅速に手続きできないかという仮説をもって、検討を行った。zkTLS の利用を、身近な事例で前後の処理の自動化・効率化とセットで検証したものであり、将来的には、ＲＷＡ（リアルワールドアセット）トークンの裏付け資産の証明といった部分で活用できる技術なのではないかといった観点で注目している。

- 株式会社 BOOSTRY より、株式会社野村総合研究所・野村證券株式会社・株式会社ディーカレットＤＣＰ・株式会社三井住友銀行との協業で行われた「国内初の決済スキームによるデジタル債の発行、及び国内初のデジタル通貨による証券決済の概念実証における協業について」のプレスリリース[2]に関し、簡単な紹介が行われた。紹介のポイントは以下のとおり。
  - ・ デジタル債として国内初のＤＶＰ決済を実現すると共に、公募債発行時の決済期間として過去最短となるＴ＋１決済を実現した。具体的には、証券会社から投資家へのデジタル債の移転において、①証券会社は、第三者に移転できない状態にロック（仮移転）し、②証券会社への資金の払込を投資家から銀行に依頼。③銀行は、ブロックチェーンから決済対

[2] プレスリリースは以下参照。
https://www.nomuraholdings.com/jp/news/nr/nsc/20250314/20250314.pdf

象のデジタル債の売買取引情報を取得して送金資金の内容との照合を行い、内容に問題がなければ、④資金交付の処理、及び⑤ブロックチェーン上のコントラクトに移転実行の署名をすることでロックを解除し本移転を実施する。このような仕組みをとることで、決済リスクを低減したＤＶＰ決済を実現した。こうしたエスクローのような仕組みを、銀行口座といった日常的に使われている手段とブロックチェーンのスマートコントラクトを連携させることで実現している点がポイント。

・ 疑似データを用いた概念実証としてではあるが、デジタル通貨を利用した場合のＤＶＰ決済も行い、オペレーションとして実行可能であることを確認した。

- 株式会社 BOOSTRY の紹介を踏まえ、参加者によるディスカッションが行われた。議論の概要は、以下のとおり。

（参加者）今回ご説明頂いたデジタル債のＤＶＰ決済は、プライマリーマーケットの事例であるが、投資家から投資家への移転となるセカンダリーマーケットの場合も、同じ手法が適用可能か。

（プレゼンタ）ご認識のとおり、セカンダリーマーケットの場合も、プレイヤーの名前が変わるだけで、適用可能である。

（参加者）本件のＤＶＰ決済において、テクノロジーの観点から何らかブレイクスルーはあるか。

（プレゼンタ）特殊な技術を用いることで導入が難しくなることを避けるため、基本的にはシンプルな取り組み且つ既存の決済システムを利用できるような形にすることに敢えてこだわった仕組みにしている。今回の仮移転の仕組みは、証券会社と投資家、決済事業者といった関係者の署名が全て揃うと、仮移転から本移転となるという、マルチシグのような分かりやすい実装となっている。

（参加者）デジタル債の権利移転について、社債原簿がブロックチェーン上にあり、その名義が変更されることで法的にも移転する仕組みになっているのか。

（プレゼンタ）社債原簿は、ブロックチェーン上にはなく、外部にある。ブロッ

クチェーン上にある保有者情報が更新（トークンが仮移転から本移転）されると、ブロックチェーン外の社債原簿上の保有者情報が即時に更新され、それを持って移転が成立する仕組みとなっている。

（参加者）従来と異なる点として、銀行が資金の払込依頼を受けた際にデジタル債と資金の決済情報を照合している。この照合作業が追加されている点、実務的に負荷が大きかったか、あるいは今後の実用化を考慮した際にボトルネックとなる可能性はあるか。

（プレゼンタ）銀行が新たに行う照合作業は、今回はマニュアルで行っており、今後本格的な実用化を考えると、システム化・自動化が必要であると認識している。

（参加者）２点質問がある。１点目は、今回のＤＶＰ決済は、新たなトラストポイントを設置せず、基本的には業務フローを工夫する形で、システム間連携を行ったという理解でよいか。２点目は、今回Ｔ＋１での決済とのことであったが、流動性準備の増加といった負担も想定される中で、今後Ｔ＋０とさらに即時性を求めるニーズはあるとお考えか。

（プレゼンタ）１点目は、ご認識のとおりで、業務フローを工夫するといったエスクローの仕組みを軸に、複数関係者の署名をもって移転するというトークン側の技術的工夫を追加することで、新たなトラストは置かない方法で実現している。２点目は、既存証券のＴ＋２の決済が変わらない中においては、デジタル債だけ即時になっても、多くの金融機関にとってはオペレーションなどの観点でコストが高くなるため、大きなニーズは見出しづらいと考える。

- 株式会社 NTT データより、「ステーブルコインの技術面での現況について」に関するプレゼンテーションが行われた。プレゼンテーションのポイントは以下のとおり[3]。

  ・ ブロックチェーン誕生の背景として、計算リソースの飛躍的な向上と遍在化が挙げられる。現代では、スペック的には一昔前の基幹系システムと同等以上の性能、リソースを備えたデバイスが、遥かに高速かつ低遅

[3] 詳細は以下のプレゼンテーション資料を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo250718a.pdf

延なネットワークに常時接続される形で広く普及している。

・ リソースが貧弱だった状況では、一か所に集約して処理内容を「保証」する中央集権管理型のシステムは合理的であったが、リソースが遍在化するパラダイムシフトによって、複数主体の合意形成で処理内容を「検証」し分散管理する新しいアプローチとしてブロックチェーン技術が発展したのは、極めて自然な帰結。

・ 2009 年に Bitcoin が始動し、2015 年に Ethereum が公開されて以降のこの 10 年間、ブロックチェーンを用いたビジネスモデルと技術は、急激に増加した。今回注目するステーブルコインは、Ethereum でトークンを発行・管理するための規格である ERC-20 から発生したファンジブルトークン、及びデジタル通貨の２つに関連する概念と認識。

・ ステーブルコインは、法定通貨と同等の価値を持つように設計された暗号資産トークンであり、①現金や現金同等物を担保とすることで価値を裏付けする法定通貨担保型、②暗号資産で価値を裏付けする暗号資産担保型、③担保資産を持たず、価格の変動リスクを経済モデルなどで調整する無担保型（アルゴリズム型）に分類される。

・ 現在、ステーブルコイン市場の９割以上は①法定通貨担保型となっており、その価値の源泉となる裏付け資産に関して、多くのケースでは、第三者による会計監査が行われレポート公開がされているものの、課題は残る。この点、ＢＩＳとＢＯＥがほぼリアルタイムで裏付け資産の情報をモニタリングする実験を行う[4]など、ステーブルコイン自体の信頼性を底上げしようとする取り組みは増えている。

・ トークン化の定義は様々あるが、高いプログラマビリティの実現を目指して「従来の伝統的決済システム上の価値」を「プラットフォーム自体が実行環境となるシステム上のトークン」に置き換えるプロセス、と考える。そうしたトークンには、単に価値を表す数字だけではなく、そのトークンがどのような属性を持っているのか、発行者や所有者が誰でどのようなものなのか、例えばＣＢＤＣなのかチケットなのか、チケットであれば転売してはならないなど、使われ方のルールもスマートコントラクトとして包み込まれている。

---

[4] 詳細は以下参照。
https://www.bis.org/publ/report_pyxtrial.pdf

・ スマートコントラクトはアプリケーションと本質的な違いはなく、ブロックチェーン技術が採用されているプラットフォーム上のアプリケーションを指す場合が多い。なお、ブロックチェーンといっても、コンソーシアムブロックチェーンの場合であれば、既存システムに類似して、責任分界は事業者間で比較的明確な一方、パブリックブロックチェーンの場合には、中央集権的な運営主体の存在が排除され、よりシステム構造は分散的となり、ノードやスマートコントラクトの提供・責任主体も不明確で、最終的には利用者の自己責任となっている点は、大きな違い。

・ ステーブルコインは、分散型台帳技術を基盤とし、その上で稼働するプログラム技術（スマートコントラクト）を使って実現されている。ブロックチェーンの基本形であるBitcoinは、ネットワーク全体があたかも一つの台帳であるかのように振る舞う分散台帳を前提としており、ここではスマートコントラクトの実行は前提としていない。2015 年にEthereum が誕生して初めて、スマートコントラクトの実行環境として、ネットワーク全体があたかも一つのコンピューターであるかのように振る舞う、分散アプリケーション基盤が登場した。

・ Ethereum等では各ノードにＥＶＭ（Ethereum Virtual Machine）と呼ばれる仮想マシンが組み込まれており、異なる環境の差異を吸収し、共通仕様のコンピューターをエミュレートして、プログラムが実行できるようになっている。ＥＶＭは、ネットワーク上のすべてのアカウント（ユーザーのウォレットアドレスやスマートコントラクトのアドレスなど）の状態を管理しており、どのノードでも同じスマートコントラクトのアドレスには同じプログラムが格納されている。例えばあるステーブルコインの送金を行う場合、送金元で秘密鍵を使ってトランザクションの生成と署名を行って処理がリクエストされると、ＥＶＭは、検証とトランスファーの関数を使って動かしていく処理を行っていく。この流れは、メモリの中に格納されたプログラムの場所を指定して、プログラムを呼び出して、メモリの中に格納されたデータを変化させるという、基本的なコンピューターの仕組みと同様。

・ Ethereum 上でトークンを発行・管理するための標準的規格として ERC-20 があり、トークンの転送や残高確認、承認などの基本的な機能を提供する関数が定義されており、ここから様々な機能が追加されることで他の多くの規格が誕生している。主なステーブルコインは、ERC-20 をベースにしつつ、保有者を限定するホワイトリスト機能など、運用リスクを軽減させる機能が追加・拡張されている印象。

・ ステーブルコインの技術的な課題として、新たなサイロ化が生じている点が挙げられる。すなわち、Ethereum への負荷集中による性能劣化及び、実行コスト高騰を背景に、他のブロックチェーンネットワークへの利用者の分散が生じ、結果、それぞれのチェーンで利用者を囲い込む傾向は避けられず、各ネットワークの規格互換性の問題や、異なる台帳間の接続性が課題となっている。

・ こうしたサイロ化を解消する方法の一つとして、全てを一つのプラットフォームの上でアトミックに処理することができるような状況を作ったらよいのでは、という Unified Ledger のアプローチがある。Unified Ledger には、完全に単一の台帳とするタイプもあれば、システム間をＡＰＩで連携するタイプなども想定されており、様々なバリエーションがある。

- 株式会社 NTT データのプレゼンテーションを踏まえ、参加者によるディスカッションが行われた。議論の概要は、以下のとおり。

（参加者）リソースの遍在化によってシステムがモノリシックな中央集権型から、レイヤーごとに役割がアンバンドルされる分散型へと変貌していき、そうした中で何かしらシステムの管理やコントロールを効かせていこうとした場合、アプリケーションが果たす役割が大きくかつ複雑になっている印象を感じた。Unified ledger といっても様々なバリエーションがある中、単一台帳の本格的な Unified ledger はチャレンジング、とのコメントがあったが、どのような点がチャレンジングか。

（プレゼンタ）システムはどんどんアンバンドルされ、マイクロサービス的に細かくしていく方法もあれば、全部一つに寄せ集めるという両極の話がでてきていると感じる。やはり、一つのシステムに全てがあるということは、技術的にはシンプルに単一障害点になる点、チャレンジングに感じる。そこの信頼性を上げていくことはもちろんできるものの、確実に動く、全く一秒の隙もなく動くというのは、たとえできたとしても高コストのものになるため、もう少し緩やかに連携させる方法もあり得るかもしれない。例えば、ネットワーク上で様々なシステムがあることを前提としつつも、共通の規格に基づいて連携することで、全体として調和を取れた、セキュリティを保たれた状態で動かすアプローチもあり得る。Unified ledger といっても、概念的には全体で一つのものとして機能するが、実際にはアンバンドリングされた様々な機能が連携することで構成されたシステムを作る方向性もあ

るのではないか。そうした観点で、次回は新しいアーキテクチャのアプローチに関してプレゼンを行いたい。

（参加者）Unified Ledger といっても、何をもって Unified であるかは定義されておらず、プロトコルは共有しているがシステム的に台帳は複数ある、といった考え方もあると理解。このような解釈の幅をもたせることで、様々な人たちの参画を促し、議論を活性化させる効果を持っていると感じている。

（参加者）カンボジアのバコンについても、当初は単一台帳で導入したが、既存の金融機関からビジネスモデルの観点で反発があり、既存の複数の台帳を連携処理する仕組みに変更しており、障害リスク以外の観点からも単一台帳に統一するハードルは存在する印象。

（参加者）Unified Ledger のバリエーションから示唆される、効率性と安全性をめぐるトレードオフや、効率性の中でもエコシステムの中でのプレイヤーが果たすべき役割については、新しい技術を将来的にどう取り込んでいくのかを議論する上で、重要な検討ポイントだと考える。

３．次回予定

次回の会合は５月 28 日（水）に開催。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ４
「新たなテクノロジーとＣＢＤＣ」
第９回会合参加者

（参加者）※五十音・アルファベット順
コインチェック株式会社
ソラミツ株式会社
大和証券株式会社
株式会社大和総研
株式会社日本証券クリアリング機構
野村證券株式会社
三井住友信託銀行株式会社
株式会社三菱 UFJ 銀行
株式会社メルペイ
株式会社 BOOSTRY
株式会社 Datachain
株式会社 JPX 総研
株式会社 NTT データ
PayPay 株式会社
SBI R3 Japan 株式会社
株式会社 Startale Labs Japan
TIS 株式会社

（事務局）
日本銀行