2025 年 9 月 29 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 10 回会合の議事概要

１．開催要領

（日時）2025 年５月 28 日（水）14 時 00 分～16 時 30 分
（形式）対面及び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

- 株式会社三井住友銀行より、本年４月に、株式会社三井住友フィナンシャルグループ・TIS 株式会社・AVA Labs, Inc・Fireblocks Pte. Ltd. と共同で発表した「ステーブルコインの事業化に向けた共同検討に係る基本合意書の締結について」のプレスリリース[1]の紹介が行われた。概要は以下のとおり。

  ・ 事業化の検討範囲は金融機関や事業者間で行われるホールセール領域。具体的なユースケースは今後事業者と議論する中で検討していくが、リアルワールドアセット（ＲＷＡ）[2]の動きが進んでいることを踏まえ、ステーブルコインとＲＷＡとの組み合わせを模索したい。複数の金融機関で協力して取り組みを進める必要性も感じている。

  ・ 共同検討自体は以前から行っていたが、米国の方で急ピッチにステーブルコインの環境整備が進んでいる状況を踏まえ、国内で関心がある事業者と繋がりやすくし、検討を一層進められるよう、取り組み内容を公表した。

- 株式会社三井住友銀行の紹介を踏まえ、参加者によるディスカッションが行われた。概要は以下のとおり。

（参加者）共同検討する上で、各社のどのような技術的特徴を活かしていくイメージか。例えば、Ava Labs が提供する Avalanche の場合、パブリックパーミションド

---

[1] プレスリリースは以下参照。
https://www.tis.co.jp/documents/jp/news/2025/tis_news/20250402_1.pdf

[2] 直訳すれば「現実世界の資産」、即ち、株式や不動産、債権、金等であるが、Web３の文脈では、これら資産を「デジタルトークン化したもの」を指すことが多い。

チェーンとして、独立したブロックチェーン環境である L1(サブネット)を各ユーザーが構築でき、例えばネットワークへの参加条件、コンセンサスアルゴリズム、利用する仮想マシン(ＥＶＭ等)、ガス代等を柔軟に設定できる。そのため、ユースケースに応じたカスタマイズ性が高い印象がある。

(プレゼンタ)最初からパーミッションレスチェーンを活用するのはハードルが高いため、認識のとおり、例えば Avalanche の特徴であるサブネット・L1 構造や高い相互運用性を活用しパーミッションドの環境を活用していく予定。また、金融機関として、安心・安全なステーブルコイン決済サービスを検討していくにあたり、Fireblocks の独自技術であるＭＰＣ-ＣＭＰ[3]は、ウォレットのセキュリティ面で活かしていけると考える。

- 株式会社 NTT データより、「価値移転プロトコル(電子現金)」についてのプレゼンテーションが行われた。概要は以下のとおり[4]。
  - 新たな決済システムを考える際に既存の台帳の仕組みを前提とすると、台帳ないしプラットフォームが持つ排他性故に、必ずサイロ化が発生してしまう。仮に、台帳に依存しない、新しい価値移転の仕組みとして、もともと現金が備えていた転々流通性・偽造防止といった性質をデジタル化するアプローチをとれば、サイロ化が生じない新しい決済手段を創出できるかもしれない。
  - ここで言う「価値移転プロトコル」は、デバイス間で価値や情報を改ざんさせずに安全に転々流通させる技術を指し、トークンが転々流通する過程には台帳は関与しない。その代わり、移転の都度、送り手と受け手の双方がトラストアンカー(認証局)から発行された証明書を用いて署名し、検証に必要な署名の連鎖をトークン自体に格納することで、当事者間でトークンの正当性が確保できる仕組みとなっている。仮にＣＢＤＣで使う場合、ＡＴＭで銀行からお金を引き出すのと同じインターフェースで、サーバウォレットからトークンを引き出すことを実現できればよい。

---

[3] 秘密鍵の断片を複数のエンティティが安全に管理し、各エンティティが協力して署名計算に参加することで、秘密鍵を復元せずにトランザクション等に署名を行う MPC(Multi-Party-Computation)技術の一つ。名称は、プロトコルの考案者(Ran Canetti、Nikolaos Makriyannis、および Udi Peled)の頭文字に由来。通常の MPC に比べて通信回数が少ないことから、コールドウォレットのような外部との通信に時間を要する環境でも利用可能とされている。

[4] 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/dfo250929b.pdf

・ 従来技術と比較した場合、「価値移転プロトコル」に準拠したシステムは、①二者間で決済が完結できる転々流通性の実現のみならず、②中央集権サーバーではなく各デバイスに処理を分散させることでの性能上限の解消、③用途制限・転売抑制・有効期の設定といったふるまいの制御、④サービス提供者は取引数の増加にともなう設備投資増強が不要、⑤通信障害時もローカル通信によりデバイス間で決済可能（オフライン決済）、⑥価値と情報のアトミックな移転が可能、といった様々な利点が考えられる。

・ 価値移転の署名・検証ロジックや秘密鍵は、改ざんや漏洩を防ぐため、これらを隔離実行環境やデバイスのセキュアエレメントで保護する仕組みをとっている。将来的には、隔離実行環境としてキャリアネットワークを活用することも展望。ユーザーが利用するデバイスからサーバーと通信するまでに必ず通過するキャリアネットワーク上に、インクルーシブコアという隔離実行環境を構築し、トークンの保持や証明書、ロジックの保護を行う仕組み。従来は、デバイス紛失の際に、その中にある価値も消失してしまう、といったことが生じがちだったが、ネットワークの中にこうした仕組みを持たせることで、こうしたデバイス固有のリスクを失くすことができる。

● 上記説明に関連する内容として、パネルディスカッションの冒頭、ソラミツ株式会社から「オフライン決済」に関するプレゼンテーションが行われた。概要は以下のとおり[5]。

・ 1990 年代後半に登場した、いわゆる「電子現金」は、カードや携帯電話の中にあるセキュアエレメントに価値を保存する仕組み。基本的にオフライン決済であり、店舗側の端末と残高を確認し足りていれば払う、という流れ。携帯の電波が無くとも、店舗側の端末に電気さえ入っていれば決済出来たので、東日本大震災の際に大変感謝された。ただし、デバイスのチップの処理性能が低く署名を連鎖させる機能は持たせられなかったため、転々流通はできなかった。また、店舗端末のログを月に１～２回集計し、二重取引等がされていないかの突合チェックを行っていたが、カード紛失等も多いため、店舗側の論理残高と市中のカード・携帯の中の残高が合わず、違算金が一部で発生していた。

・ 現在関与している海外ＣＢＤＣ実証実験の一つでは、インターネット環境が整っていない地域であるため、オンラインＣＢＤＣとオフラインＣＢＤＣを一つのデバイスで利用できるハイブリッドなアーキテクチャを検討。セキュ

[5] 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/dfo250929a.pdf

アエレメントの利用が必須であるためデバイスが一部限定されることや違算金発生の課題は残るものの、デバイスの処理性能が向上していることから、ブロックチェーンで署名の連鎖と二重取引や偽造を検知する仕組みを構築できており、オフラインでの転々流通性を実現している。

- 株式会社 NTT データ、ソラミツ株式会社のプレゼンテーションを踏まえ、パネリスト[6]含む参加者間でディスカッションが行われた。概要は以下のとおり。

（参加者）トークンとトランザクションの関係について質問がある。トランザクションの中にトークン移転のメッセージや属性が記録されており、トークン移転毎に送り手と受け手の双方の証明書を用いて署名する、といった認識であっているか。

（プレゼンタ）ご認識のとおり。属性情報の中には、発行から還収するまで変わらない永続的なものと、トランザクションに固有のものが存在する。例えば、店舗であればトランザクション固有の属性情報を得られ、地域通貨の発行者であれば、転々流通後に還収されたトークンを検証することで、地域のエコシステムにおける匿名の金流情報を得ることができる。

（参加者）二重取引はどのように防止しているのか。

（プレゼンタ）耐タンパ性を備えたデバイスを利用することで、改ざんが困難である性質を持っているほか、還収時に発行の際に付与されたシリアル・ナンバーが既に還収済になっていないか確認することで、事後的に二重取引は検知する仕組みを備えている。

（参加者）プライバシーの観点で質問がある。発行者は還収時に移転情報を得ることができるとの説明だったが、ユーザーも移転情報を把握することは可能なのか。ユーザーが自分の前に誰がトークンを持っていたのかが見えてしまうとプライバシーの観点で好ましくないと考えるが、属性情報の参照権限はどのように制御されているのか。

（プレゼンタ）ユーザーは、検証の過程で、過去の匿名の証明書をみることはできるが、証明書と本人性を紐づけることはできない。そういった紐づけができるのはトラストアンカーとして限られた機関のみとなる前提である。すなわちユーザー

[6] セコム株式会社、ソニー株式会社、ソラミツ株式会社、大日本印刷株式会社がパネリストとして登壇。

はトークンの移転情報を把握することは可能であるが、その情報に紐づく個人は特定できない仕組み。

（参加者）将来的な価値移転プロトコルの利用イメージはどのようなものか。例えば国民すべてに利用されているものなのか、もしくは事業者間の移転のみ、といった限定的なイメージであるのか。

（プレゼンタ）プロトコルと名付けていることからも推察されるかもしれないが、インターネットが普及した際と同じように出来ないかと考えている。ネットワーク技術の進展と合わせ、誰もが使いやすい状態をつくっていく方向性を考えている。

（参加者）プラットフォームではなくプロトコルでという説明を聞き、インターネットにおける標準通信プロトコルであるＴＣＰ／ＩＰのような使われ方をイメージした。ほぼ公共財的なプロトコルとして存在し、民間事業者はそれを活用して多様なサービスを生み出していく姿を想像した。

（参加者）トークンの移転回数に上限回数を設ける場合、上限回数に達したトークンはどういった処理を行うのか。金流分析への活用を考慮した際に上限回数が少ないとデータ量の観点から有効な分析ができない可能性があると考えるがどうか。

（プレゼンタ）上限に達したトークンは、支払いには利用できない状態で発行元に自動で返却される仕組みを、ウォレットが備えるイメージ。上限回数については設計次第。データサイズ等を踏まえ、ユースケースに応じて適切な回数を検討していけばよいと考える。

（参加者）資金だけではなく、株式等のＲＷＡのトークン化にも、ご提案のプロトコルは応用可能か。

（プレゼンタ）トークン化のプロセスにおいては適用可能。ただし株式保有者把握のリアルタイム性や株価等の投資家向け情報、といった追加的な仕組みは別途準備をする必要。

（参加者）サイロ化の解消を実現するにあたっては、実際にその技術やアイデアにどれだけみんなが乗っかれるか、といった観点でのフィージビリティも検討していく必要。一足飛びに皆が同じプロトコルに移行してくれることは現実的には難しく、既存の仕組みと併存しながら普及していく必要があると考えるが、どうか。

（プレゼンタ）これまで台帳システムを利用してきた大規模かつクリティカルな決済

システムが、価値移転プロトコルに移行する判断は難しいかもしれない。ただ、仮に移行した場合は、システム構築にかかるコストを大幅に削減できるため、費用対効果の観点で採用されることは将来的にあり得る。新しいシステムを構築しようとする際に、現在だとブロックチェーンやトークン化、ステーブルコイン系の技術が注目されているため、一旦そうしたトレンドは続くと思うが、そうした技術を使ってみて、やっぱりサイロ化が弊害になるよね、ということが確認されていくフェーズが来た場合、価値移転プロトコルが採用されやすくなる可能性もある。採用事例が徐々に増えていけば、ネットワーク効果を伴い、今のインターネットのようにみんなが自然と価値移転プロトコルの上に載ってくるという流れができたらと考える。

（参加者）一度プロトコルを制定し長く運用することを考えると、プロトコル自体への機能追加や修正も必要となってくると考えられるが、バージョンアップはどの程度必要になってくる想定か。

（プレゼンタ）プロトコルとして切り出すのは、正しく価値移転ができているかの検証という極めてシンプルなものであり、頻繁なバージョンアップは想定していない。インターネットのＴＣＰ／ＩＰもアップデートはしてきたので、そのやり方は参考になると考える。

（プレゼンタ）価値移転プロトコルが持つ、転々流通性や決済コスト削減、属性情報の付与といった利点は非常に大きなポテンシャルを感じている一方で、普及にあたっては、関係者からみて敵だと思われない仕組みや見せ方を検討し、全体のエコシステムの中で Win-Win の構造を考えていく必要。

（参加者）普及に関しては、既に加盟店を開拓している決済事業者と上手く連携することも一つの選択肢。

（プレゼンタ）価値移転プロトコルは、サービスレイヤーの下のレイヤーに位置づけられ、まさにインターネットの上のサービスレイヤーにプラットフォーマーが現れている構造と同じである点には留意が必要。価値移転プロトコルを採用することで、その上のサービスレイヤーで行われていた加盟店開拓が無駄になることはなく、むしろより新しい価値提供サービスができるようになる、といった目線で協業が増えていくことが望ましい。

（参加者）隔離実行環境やセキュアエレメントの技術自体は以前から普及しているが、そこにインクルーシブコアという通信ネットワーク技術を組み合わせようとしている点が、これまでなかった新しさ。

（プレゼンタ）価値移転プロトコルの普及の観点で、ユーザー目線ではどのような考慮事項があるか。

（プレゼンタ）インターオペーラビリティが最も重要。日本の場合、様々な決済手段がある中で、店舗によって利用できない決済手段があったり、決済手段同士の価値の移転ができない、もしくは複雑となっているケースがみられる。価値移転プロトコルが採用されれば、そうしたサイロ化を解消するインターオペーラビリティを提供できるのかもしれない。店舗目線では、決済手数料の安さや売上代金の入金サイクル短縮化も重要な観点。

（参加者）ソラミツの海外ＣＢＤＣの実験について、オンラインＣＢＤＣとオフラインＣＢＤＣを一つのデバイスで利用可能との説明があったが、ユーザーがオンラインＣＢＤＣを利用するつもりであったのに誤ってオフラインＣＢＤＣを利用するといったことも考えられるため、ＵＸの観点で工夫を検討するとよいかもしれない。

（プレゼンタ）仮に、価値移転プロトコルが普及していった姿を想像すると、これまで決済事業者や店舗のシステムに蓄積されていた購買履歴等の決済データが、個々人のデバイスに蓄積されていくことになる。ユーザーの情報を保持することには相応のリスクやコストが伴うことから、事業者自身はユーザー情報を保有せず、ユーザーが自らデバイス等に蓄積された情報を必要に応じて事業者に提供し、最適なサービスを受けるといったユーザードリブンマーケティングという形も考えていけるのではないか。

（参加者）将来的にはＡＩエージェントのような存在がユーザーのデバイスに蓄積された情報をもとに様々な判断を行う世界観もあるかもしれない。

（参加者）ユーザードリブンマーケティングやＡＩエージェントに関しては、ブロックチェーン技術においても、その活用検討が盛んになっている。データはユーザーのデバイスに保持しつつ、チェーン上で、アクセス権を付与したＡＩや事業者に対しては情報を透過し、必要に応じてゼロ知識証明を用いて内容を秘匿化するといったアプローチに取り組んでいる。現状、ゼロ知識証明には処理性能に課題があるが、技術的な改善が今後進んでいくことに期待。

（参加者）価値移転プロトコルの実運用に際して、既存のスマートフォンやウォレットの機能で十分なのか、あるいはまだ不足する部分はあるのか。

（プレゼンタ）全ての条件を満たしているとは言えないが、ver．１を作るには十分な状態と考える。もっとも、これまで説明してきたインクルーシブコアや、先ほど言及のあったゼロ知識証明といった、様々な機能を追加していく余地は大きい。

（参加者）価値移転プロトコルにおける匿名性や限度額について、どのように考えるか。

（プレゼンタ）匿名性に関しては、ＡＭＬ／ＣＦＴとのバランスが重要。本人と属性情報を紐づけ可能である主体を、証明書の発行業務を担うトラストアンカーのみに限定することが、一つの方向性と考える。上限額に関しては、発行する証明書のレベルに応じて区分を設ける方法が考えられる。

（参加者）プラットフォームからプロトコルへ、というキーワードは今回の大きな学び。技術、制度、実務面の議論をバランスよく徐々に粒度を高めていくことが重要と感じた。引き続き、様々な観点から議論を行ってまいりたい。

３．次回予定

次回の会合は 10 月 14 日（火）に開催予定。

以　　上

別紙

ＣＢＤＣフォーラム ＷＧ４
「新たなテクノロジーとＣＢＤＣ」
第 10 回会合参加者

（参加者）※五十音・アルファベット順

株式会社イオン
コインチェック株式会社
株式会社ことら
株式会社静岡銀行
セコム株式会社
株式会社セブン銀行
ソニー株式会社
ソラミツ株式会社
大日本印刷株式会社
大和証券株式会社
トヨタファイナンシャルサービス株式会社
株式会社トレードワルツ
日本電気株式会社
日本アイ・ビー・エム株式会社
株式会社日本証券クリアリング機構
日本マイクロソフト株式会社
野村證券株式会社
株式会社野村総合研究所
東日本旅客鉄道株式会社
株式会社日立ソリューションズ
日立チャネルソリューションズ株式会社
株式会社マネーフォワード
株式会社みずほ銀行
三井住友海上火災保険株式会社
株式会社三井住友銀行
三井住友信託銀行株式会社
株式会社三菱 UFJ 銀行
三菱 UFJ ニコス株式会社
株式会社横浜銀行
楽天ペイメント株式会社
株式会社りそなホールディングス
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
NRI セキュアテクノロジーズ株式会社
株式会社 NTT データ
株式会社 NTT ドコモ
PayPay 株式会社
SBI R3 Japan 株式会社
株式会社 Startale Labs Japan
TIS 株式会社
TOPPAN エッジ株式会社

（事務局）
日本銀行