2025 年２月３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５回会合の議事概要

１．開催要領

（日時）2024 年７月４日（木）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

- 株式会社 JPX 総研より、「台帳データモデルに関する考察」に関するプレゼンテーションが行われた[1]。プレゼンテーションのポイントは以下の通り[2]。

  ・ 中央管理型の台帳システム構成（中央銀行が単一の台帳を管理する構成）における送金機能を対象に、各種制限（保有額や取引額および取引回数をユーザー単位で制限）を課すことを前提として、口座残高型、固定額面トークン型およびＵＴＸＯ型のデータモデルを比較。

  ・ 性能（スループット・レイテンシ）について、固定額面トークン型やＵＴＸＯ型は、更新対象レコード数が多くなる傾向にあることやユーザー単位の残高計算が必要であること、両替・お釣りといった処理が別途必要となる場合があることによって、口座残高型より劣る可能性を指摘。

  ・ 性能（並列処理性）について、送金の実行前に各種制限チェックを都度行う前提の場合、ユーザー単位で排他制御を行う必要が生じるため、モデル間の差異はないと評価。
  　ただし、各種制限チェックに関し、送金の都度ではなく事後的に行うなど前提を変える場合には、評価が変化する可能性にも言及。

---

[1] 本プレゼンテーションは、これまでの会合で、台帳データモデルの特性はシステム構成など前提の置き方で異なってくるとの指摘を踏まえ、前提を明らかにした上で台帳データモデル比較のプレゼンテーションを行う有志を募った結果、実現したもの。

[2] 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/dfo250203a.pdf

・ 信頼性（セキュリティリスクへの耐性・取引のアトミック性（整合性））について、モデル間に差異は見当たらないと評価。

・ 拡張性（追加サービスとの親和性）について、「お金に色を付ける」ユースケースがあれば固定額面トークン型が優位となる可能性を指摘。

・ 拡張性（実装容易性）について、固定額面トークン型の場合、トークンの額面や粒度の設定、送金時におけるトークン選択アルゴリズムの詳細な検討が必要となることから、実装難度が上がる可能性を指摘。

- ソラミツ株式会社より、「ＣＢＤＣへのＤＬＴの応用可能性」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通り[3]。

・ カンボジアのバコンは、既存の決済サービスを活かすといった点を考慮し、民間金融機関の債務がリアルタイムに移転する形をとっている。システムの運営は中銀が行い、中銀は個人情報を持たず、民間金融機関が本人確認を行う役割分担となっている。取引上限金額に応じ本人確認のレベルを変えており、1 日 250 米ドル（または 100 万リエル）を上限とした場合、電話番号のみで口座開設が可能となっている。

・ バコン導入当初は、中銀が統一アプリを提供する形をとったが、民間金融機関からの反発があり、加盟店開拓が進まなかった。このため、各民間金融機関が既存のアプリケーションを利用する形にしながらも、ＱＲコードの規格は統一し、ＡＰＩも共通化することで、アプリケーション間の互換性をとる仕組みに変更。こうした取り組みが奏功し、加盟店開拓が進むようになった。また、現在ではタイやベトナムといった近隣諸国とのクロスボーダー決済も可能となっている。

・ カンボジア以外では、ラオスやソロモン諸島といったアジア・大洋州島嶼国等に対し、ＣＢＤＣの実証実験や導入に向けた支援を行っている。特に島嶼国においては、現金の輸送コストが高く、出稼ぎも多いため、ＣＢＤＣやクロスボーダー送金のニーズが高い。

・ 当社が開発し現在は Linux 財団が管理するパーミッションド・ブロックチェーンの Hyperledger Iroha は、口座残高型データモデルで、データセパレーションとアクセスコントロールによって、プライバシーを柔軟に保護できる特徴を持つ。例えばカンボジアのバコンの場合、

[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/dfo250203b.pdf

Hyperledger Iroha のオンチェーンでは個人情報を取り扱わない形で残高や取引履歴を記録し、それ以外のビジネスロジックや個人情報等のデータベースはオフチェーンで取り扱っている。

・ ＣＢＤＣへのＤＬＴの応用を検討する際には、処理能力をどのように確保していくかがポイント。Hyperledger Iroha v2.0 では、合意形成に参加するノードを絞り、インメモリデータベースを利用することなどの工夫を施すことで処理の高速化を図っている。例えば１億人を超える規模の国にＤＬＴ基盤を採用する場合には、仲介機関別やエリア別にＤＬＴを階層化したり、処理によって中央集権的なデータベースとＤＬＴを使い分ける（残高管理はＮｏＳＱＬといった中央集権的データベースで処理を高速化し、履歴管理はＤＬＴを用いセキュリティを高めていく）といった工夫も考えられる。規模が小さく、クロスボーダー取引が多い島嶼国においては、低コストで導入できる共通プラットフォームの需要が高いことから、パブリックブロックチェーンの仕組みも活用したハブ・チェーンの開発を行っている。

３．ディスカッション

● 株式会社 JPX 総研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、以下の通り。

（参加者）拡張性における追加サービスとの親和性の評価項目において、「例えばお金に色をつけ資金使途ごとに管理するようなユースケースを考えると、トークンごとにデータを管理する固定額面トークン型が最も優れているのではないか」とご説明いただいたが、具体的な例としては、特定の地域のみで利用できる地域通貨や利用用途が限られる助成金のようなユースケースが考えられるか。

（プレゼンタ）挙げていただいた地域や利用用途を特定するようなものをイメージしているが、他にも多くのユースケースがあり得ると考える。なお、ＵＴＸＯ型や口座残高型であっても工夫次第で同様のユースケースへの対応自体は可能と思われるため、資料上「▲？」「〇？」のように特に暫定的な評価であることを表現した。

（参加者）第３回会合での NTT データのプレゼンテーションとの違いという観点では、システム構成の前提が分担管理ではなく中央管理に変わっている

ことから、どのデータモデルであっても、全ての取引が中央システムを介して処理する形となっていると認識[4]。こうした想定のもと、各種制限をユーザー単位で厳密に行うとする場合、固定額面トークン型やＵＴＸＯ型を利用しても、ユーザー単位での排他制御やトークンの合算処理が必要となるため、トークン型で言われる複数処理を同時に行える並列処理性は損なわれる可能性をご指摘いただいた。一方で、各種制限の業務フローの工夫次第では、いわゆるトークン型の並列処理性を活かせる可能性も、同時にご指摘いただいたと理解している。

　また固定額面トークン型やＵＴＸＯ型の場合、初期設定としてどれくらい細かくトークンの粒度をもっていくか、どのようなアルゴリズムで最適な消費トークンを選定するのかといった検討は、実装時に別途必要となるため、実装の複雑性が増す可能性もご指摘いただいた。並列処理性という観点では、トークンの粒度を細かくすればよいように考えられるものの、粒度を細かくしすぎると必要なトークンの選定に時間がかかるなど、性能面に負の影響を与える可能性もあるかもしれず、単純ではない感触。

（プレゼンタ）データモデルの検討の際に、そもそも並列処理性にどの程度重きを置くべきか、も議論の余地があるように考える。台帳システムが中央管理の構成を想定した上で、個人のエンドユーザー間の送金のみユースケースとして考えた場合には、ある個人が複数の人に同時に大量の支払いを行う場面はそこまで生じないとも思われ、データモデル選択において、並列処理性はそこまで大きな要素とはならない可能性もある。

（参加者）固定額面トークン型に関し２点質問がある。１点目が、トークンの種類は単一と複数いずれの想定であるか。２点目は、所有者がいないトークンはあり得るか。

（プレゼンタ）１点目については、複数の額面を想定している。説明資料上、

---

[4] NTT データのプレゼンテーションにおける分担管理アーキテクチャの場合、口座残高型であると同一仲介機関内の取引は中央システムを介さず処理することができる一方、ＵＴＸＯ型であると、トークンの真正性チェックのため中央システムを介する処理が全ての取引で必要となる。このため、ＵＴＸＯ型の方が、全体としてのスループットやレイテンシが劣化する可能性が指摘されていた。議事概要やプレゼンテーション資料は以下を参照。
議事概要：https://www.boj.or.jp/paym/digital/d_forum/dfo240816b.pdf
プレゼンテーション資料：https://www.boj.or.jp/paym/digital/d_forum/dfo240816a.pdf

例示として100円トークン、500円トークン、1000円トークンと記載しているが、デジタルということで２のべき乗（１円、２円、４円、・・・）の額面、といった世界も考えられるかもしれない。単一の額面、例えば10円トークンだけのような設計はここでは考えなかった。２点目については、ＣＢＤＣは中央銀行の負債として仲介機関に発行され、仲介機関からエンドユーザーの預金との交換で払い出される前提で考えると、トークンは仲介機関もしくはエンドユーザーのいずれかに必ず紐づく形になり、所有者がいないトークンは想定されないのではないか。

（参加者）固定額面トークン型やＵＴＸＯ型において、利用するトークンの選択についてアルゴリズムを工夫しないと、トークンの細分化につながり運用が難しくなると考えており、プレゼンテーションでのご指摘の通りと感じた。

　追加サービスとの親和性に関しては、例示いただいたお金に色を付けるようなケースでは、結局のところ、台帳システムと何か外のシステムとの連動、ということになるため、アプリケーションで制御するイメージであり、データモデルにおける差はそこまでないのではないかという感触。

（プレゼンタ）いずれもご指摘の通り。追加サービスとの親和性の評価に関しては、前述の通り、どのデータモデルでも工夫次第で実現できるのではと考える。単純に、お金に色を付ける場合、お金が主語になるため、固定額面トークン型やＵＴＸＯ型の方が、口座残高型よりは作り込みが容易になるのかなと思った程度の感触を記載させていただいた。

（参加者）固定額面トークン型の場合、送金の都度、両替とお釣りの処理が相応に発生する可能性が高くなるため、実装上の検討事項となるだろう。ブロックチェーンの文脈にはなってしまうが、例えば口座残高型であっても、グラフ構造を用いて関係する取引が多い口座グループとそうでないグループごとにチェーンを分割するなど、工夫次第で並列処理性は高められるのではないかと考える。

- ソラミツ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、以下の通り。

（参加者）２点質問がある。１点目は、「バコン導入前は複数存在していたＱＲコードの規格を、バコン導入後、ＫＨＱＲに統一された」と説明いただ

いたが、民間事業者からコンセンサスを得るために、どのような工夫があったかお伺いしたい。２点目は、バコンによるクロスボーダー取引についてバコンシステムへの接続のための他国（タイ、ベトナム、マレーシア等）事業者のアプリケーション開発コストが相応にかかると考えるが、いかがであるか。

（プレゼンタ）１点目については、ＱＲコードの普及について先行している民間事業者から賛同を得るのに時間がかかったものの、カンボジア中央銀行が、ＱＲコードの規格が統一されていないと国全体の発展に影響が出るとして、丁寧に関係者への説明・説得を行ったことで、規格の統一が実現できたと聞いている。２点目については、国の識別や為替レート計算といった共通機能を持つバコンシステムに常時接続するペイメントゲートウェイを他国事業者にも開放しているため、各事業者のアプリケーションは一切変更する必要がなく、開発負担が少ない仕組みとなっている。

（参加者）２点質問がある。１点目は、「バコンは民間金融機関の債務として発行される」と説明いただいたが、破綻した際の預金保険のような保証制度はあるのか。２点目は、自国通貨の流通強化がバコン発行の理由の一つであるか。

（プレゼンタ）１点目については、預金保険機構のような保証制度はない認識であるが、破綻した民間金融機関が保有するバコンについては、中央銀行が当該バコン残高を他の民間金融機関に移すことができるためユーザーは継続してバコンを使い続けることが可能、と聞いている。２点目については、ご指摘の通り、それがカンボジア中央銀行のバコン導入の目的の一つであったと推察される。自国通貨リエルは、紙幣にすると１ドル 4,000 リエルと非常にかさばるため、デジタル化することで利便性が上がり、実際にリエルの利用率が高まっているという話を聞いている。

（参加者）２点質問がある。１点目は、初回会合でも指摘された、ブロックチェーンのトリレンマ（分散性・スケーラビリティ・セキュリティの間にトレードオフが存在）について、それを乗り越えるような試みをされてきたと理解しているがどうか。２点目は、「Hyperledger Iroha の ver1.x から 2.0 にアップデートする中で、ver1.x では処理能力（ＴＰＳ）が 2,000～3,000 であったが、ver2.0 ではそれを大きく上回る 20,000ＴＰＳを目標としている」とご説明いただいたが、どのような修正が性能向上に寄与した

のか。

（プレゼンタ）１点目については、ブロックチェーンのトリレンマはやはり存在しており、そうした構造を踏まえ、多くの中央銀行からは、ガバナンスは自分たちで持ちたいという要望を聞いているため、自分たちとしては、ベースはパーミッションドのブロックチェーンという形で多少分散性を犠牲にしてスケーラビリティ・セキュリティを上げていく取り組みをしている。２点目については、基本的に全てのバリデーション処理をインメモリデータベースで処理する形に変更したことが、性能向上に大きく寄与している。

（日本銀行）様々な前提を置きそれらを明らかにした上で、性能面の評価をいただき、非常に参考になった。このような形で少しずつ精度をあげた議論を本ＷＧの皆様と出来ればありがたい。

４．次回予定

次回の会合は９月 12 日（木）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５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
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 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

（事務局）
日本銀行