

2024年4月4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1回会合の議事概要

1. 開催要領

(日時) 2024年1月30日(火) 14時00分～16時30分
(形式) 対面形式及びWeb会議形式
(参加者) 別紙のとおり

2. プレゼンテーション

- 事務局から、「【新たなテクノロジーとCBDC】ワーキンググループ(WG4)について」の資料¹に基づき、説明を行った。
- SBI R3 Japan 株式会社より、「UTXOモデルの特徴理解」の資料²に基づいて、プレゼンテーションが行われた。

3. ディスカッション

- 上記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。

【検討の進め方に関する議論】

(参加者) 最初に、本WGの議論の対象の全体像を確認し、その全体像の中のどの部分から議論を始めるかについて、参加者の認識を揃えると良いのではないかと。

(日本銀行) 他のWGは、CBDCシステム(バックエンド・フロントエンド領域)そのものや、CBDCと他の決済手段や資産との共存といったテーマを複数のWGでカバーし、基本的に現在活用されている技術を踏まえて

¹ https://www.boj.or.jp/paym/digital/d_forum/dfo240404b.pdf 参照。

² https://www.boj.or.jp/paym/digital/d_forum/dfo240404a.pdf 参照。

議論している。一方、WG 4は単一のWGでこの範囲を検討対象としつつ、将来的に活用されうる技術に着目し、必ずしも現在の技術的な前提や制約を意識せずに議論する想定である。

検討の進め方としては、まずはバックエンド領域から議論を開始し、議論の進捗をみながら、他の決済手段や資産との共存やフロントエンド領域の検討も進めていく予定である。

バックエンド領域についても様々な構成要素や論点が考えられるが、まずは、CBDCシステムの基盤となる台帳を取り上げ、その性能向上策にフォーカスをあてたい。これは、我々の「概念実証」において、台帳の中の特定口座にトランザクションが集中する際にパフォーマンス低下がみられる点が大きな課題として認識されたためである。

CBDC台帳システムの性能向上策については、データ更新時のロック範囲や更新の仕方に関する工夫、データベース機能や実装上の工夫のほか、口座に残高を紐づける形態とは異なるデータモデル、たとえばUTXO (Unspent Transaction Output) モデルなどを採用することなど、様々な技術的アプローチの可能性があると考えられる。その中で、本WGでは、まずデータモデルについての検討から開始したい、と考えている。

(参加者) 議論の前提としてCBDCシステムの構成について解像度を上げておくと、実質的な議論につながるのではないか。たとえば、システムが分散しているところにUTXOモデルを採用しようとする、このモデルのメリットが享受できない可能性があるとの印象がある。

(日本銀行) 議論の対象を狭めすぎないようにするために、前提を一つには絞らずに、たとえば、システム構成についてデータベースが単一か分散管理されているかといった複数のシナリオを前提とし、それぞれについて議論するというアプローチはありうると思われる。こういった前提を置くかについて、交通整理していきたい。

【台帳のデータモデルに関する議論】

(参加者) SBI R3 Japanのプレゼンテーションにあった、バランス型、トークン型、UTXO型の3つのデータモデルについて、それぞれの長所・短所は、台帳管理のあり方が集中か分散かなどによって変わり得るのではないか。

(参加者) 各データモデルの長所や短所は、台帳の持ち方等のシステム構成の違いで変化する可能性はあり、論点の一つと考える。

(参加者) 米国 Project Hamilton やデジタルユーロ・プロトタイピングは、分散環境ではないシステムで UTXO モデルを使ったパターンだと認識している。仮に、複数のシステムあるいは複数の主体がそれぞれデータを分割して保有するといった分散環境を前提とすると、UTXO を使うメリットを享受できない可能性がある。

(参加者) データが分散されていても、トランザクション情報のハッシュだけ中央に持ってきて存在性検証を行う形にすれば、UTXO のメリットは引き続き享受できる仕組みは作れるのではないか。

(日本銀行) SBI R3 Japan のプレゼンテーションにあったバランスモデルであっても、データ更新の方法を工夫することなどにより、UTXO モデルが得意とする並列処理性が一定程度確保できるのではないかと指摘は示唆的である。シャーディングも含め、様々なアプローチの性能向上策を比較していくということだろう。

(参加者) SBI R3 Japan のプレゼンテーションにあった分散システムにおけるユニークネスコンセンサス（取引毎整合性）について、時点ごとと取引ごとに整合性を確認する方法が挙げられているが、一般的な DLT では時点ごとで行われている印象がある。取引ごとに整合性を確認するメリットは何か。全体の整合性をとろうとした場合には、どのように対応していくことができるかと考えるか。

(参加者) 取引ごとの整合性確認の場合、無関係な取引のデータが含まれないため、たとえば、不整合が検出された時に遡及して訂正しなければならない範囲が小さい、といったことはメリットの一つと考える。

(参加者) UTXO モデルは設計次第でバランスモデルやトークンモデルに変化可能という説明について付言すると、たとえば UTXO モデルでの取引データを蓄積しておき、残高を知りたいときに足し上げることで口座ごとの残高を把握できる、といった意味である。

【ブロックチェーン技術に関する議論】

(参加者) ブロックチェーンに関連して、スケーラビリティ、セキュリティ、分散性は、全てを高度に成り立たせることが難しいというトリレンマが語られることがあるが、おそらく台帳システムの方向性としては、スケーラビリティやセキュリティを重視した上で、ある程度中央に集中させる技術を採用していくのかなという感触を持っている。もっとも、ブロックチェーンに関してスケーラビリティを高める新たな技術も出てきているので、今後ご紹介できればと考えている。

(参加者) ブロックチェーンの中には、履歴を残して耐改ざん性を維持しつつ、高いスケーラビリティを実現するような技術が出てきているので、今後の会合でご紹介していきたい。また、プログラマビリティなど性能面以外の論点もあると思うので、取り組みの実例を紹介しながら、整理していけたらと思う。

(日本銀行) ブロックチェーンの関連技術を含め、新しい技術を学んでいくことは、将来の決済システムを考えるに際して有意義と考える。既存の技術との組み合わせも含め、様々な観点から、最近の技術動向に関する議論を続けられたらと考えている。

(日本銀行) 今回は、様々なトレードオフの関係がある中で、バランスをどのように取っていくかといった議論が多く、非常に興味深く聞かせていただいた。今後も本WGの皆様と闊達な議論を進めて参りたい。

4. 次回予定

次回の会合は3月13日(水)に開催。

以上

CBDCフォーラム WG4
「新たなテクノロジーとCBDC」
第1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

セコム株式会社

ソラミツ株式会社

大和証券株式会社

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

SBI R3 Japan 株式会社

株式会社 Startale Labs Japan

(事務局)

日本銀行