2024年7月3日
日本銀行決済機構局

C B D Cフォーラム WG 4
「新たなテクノロジーとC B D C」
第2回会合の議事概要

1. 開催要領

(日時) 2024年3月13日(水) 14時00分～16時30分
(形式) W e b会議形式
(参加者) 別紙のとおり

2. プレゼンテーション

- SBI R3 Japan 株式会社より、「U T X Oモデルの将来」の資料¹に基づいて、プレゼンテーションが行われた。
- コインチェック株式会社より、「昨今のデータモデルと分散台帳のC B D Cへの利用可能性」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

- SBI R3 Japan 株式会社のプレゼンテーションを踏まえ、U T X Oモデルと口座残高型モデルの特徴について、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) パフォーマンスの観点から口座残高型とU T X Oを比較すると、U T X Oは並列処理しやすい傾向はあるものの、粒度が細かすぎると残高計算のオーバーヘッド(間接的に必要となる計算量)が高くなる可能性があるほか、処理集中を完全に失くすことはできないと考える。また、口座残高型であっても、レコードを分割したり、データを追記していくなどの工夫を施すことで、並列処理性を高めることはできると考えられる。このよう

¹ https://www.boj.or.jp/paym/digital/d_forum/dfo240703c.pdf 参照。

² https://www.boj.or.jp/paym/digital/d_forum/dfo240703b.pdf 参照。

にシステム構成や処理の実装の仕方次第であり、無前提にUTXOに性能面の優位性があるとは必ずしも言えないのではないか。

(参加者) バランス(口座残高型)でも、工夫次第でUTXOと同様の利点を享受可能というのは、ご指摘のとおりだと思う。もっとも、口座残高型では、どのようにレコードを分割するのが効率的かなどを考える必要がある。

(参加者) 課題として指摘されたスマートコントラクトの実行環境のセキュリティについては、例えば、スマートフォンなどのハードウェアデバイスが実行環境である際に、環境が信頼できる状況かを検証するアテストーションといった技術の活用を考えていくことになるのだろう。

(参加者) 鍵を失くしたユーザーが鍵の再発行を任意で行うことはできないため、当社では、マルチシグネチャーで実現している。本人立ち合いのもと錠前屋さんが来て、家の鍵と錠を交換するようなことをブロックチェーン上で行う形となっている。管理者に権限が集中しないよう牽制が働くような実装となっているほか、鍵を紛失したユーザーの本人確認を民間銀行が再度行う仕組みとなっている。

- コインチェック株式会社のプレゼンテーションを踏まえ、データベース技術やデータモデルの特徴について、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。

(日本銀行) データベース技術に関して、NoSQL データベースといっても、データモデルはキーバリューストアからグラフベースなど様々で、製品によっても特徴は異なってくる、というご指摘は示唆的である。

また、ブロックチェーン技術におけるデータモデルに関して、プログラマビリティの観点でブロックチェーンの評価に差があるが、どのような背景で差が生じているか伺いたい。

(参加者) 評価の差については、データモデルの差というよりも、プラットフォームの理念やコミュニティがプログラマビリティをどれだけ意識しているかが関係している。例えばビットコインの場合、そもそもプログラマビリティを目指したプラットフォームやコミュニティではなく、UTXOという具体的なデータモデルとプログラマビリティを結び付けて語ることは

難しい印象がある。一方、イーサリアムの場合、スマートコントラクトの実行環境であるEVM (Ethereum Virtual Machine) が存在し、プラットフォームの理念としてプログラマビリティを高めることが意識されている印象がある。もっとも、ビットコインについても、プログラマビリティを高めようとするプロジェクトも増えており、今後評価は変化していく可能性はある。

(日本銀行) CBDCと他の決済手段との共存や、他の資産との交換容易性を考えていく意味で、示唆に富むご説明をいただいた。様々なデータモデルに対応しながらサービスを提供するうえで、UTXOや口座残高型といったデータモデルの違いはどのように吸収しているのか。

(参加者) UTXO型であっても、ユーザーに紐づいた残高がすぐ認識できるよう、常に足し合わせているなどしている。

(参加者) 例えば、ビットコインから円に交換にする場合、交換所を利用するユーザー目線ではすぐ交換が完了しているように見える。実際には、コンセンサスの確定を待つ必要があると考えられるが、どのように確定判断を行っているのか。

(参加者) ブロックがいくつ生成されれば事実上の確定と見なせるかはチェーンごとに異なるが、当方で事前に判断基準を定めユーザーに提示している。例えば、あるチェーンでは、この確率だったら弊社としてリスクを許容するというブロック数を定め、その基準の数を超えたら確定の判断をしている。

(参加者) 例えば口座残高型の場合、残高を認識しやすく、その分確定までの時間が早くなるなど、データモデルによって、確定までの時間のかかり方に違いはあるか。

(参加者) 確定までの時間のかかり方は、データモデルというより、コンセンサスアルゴリズムの種類や他の設計要素が影響しているのではないか。例えば、トランザクションの確定については、確率的に決まるものと、決定論的に決まるものがあり、後者の方が中央集権的に判断するため確定までの時間が早くなる傾向はあるように感じる。

4. 次回予定

次回の会合は4月10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2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

PayPay 株式会社

SBI R3 Japan 株式会社

株式会社 Startale Labs Japan

(事務局)

日本銀行