

2024 年 8 月 16 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 3 回会合の議事概要

1. 開催要領

(日時) 2024 年 4 月 10 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

- 株式会社 NTT データより、「C B D C に関する性能面の課題と対応の方向性」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¹。
 - ・ 口座残高型における、更新処理集中時のレコードロックに伴う性能劣化に対しては、トランザクションを集約し、口座に対する更新処理数を削減することで、影響を緩和することが可能。
 - ・ 取引のアトミック性を維持したり、サーバ間で整合性のとれた処理を実現するためには、仲介機関ネットワークで一元的に処理状況をモニタリングするといったトラザクションを保証する工夫が重要。
 - ・ 必要な性能拡張は D B サーバの水平分割（シャーディング）で対応することが可能。ただし、データ量やアクセス量に偏りがでないよう、負荷の均等分散やリバランスといった工夫が重要。
 - ・ 上記の対応・工夫を施した口座残高型と U T X O 型を比較すると、更新処理集中時の並列処理性は同等となる。
 - ただし、台帳を中央システムと仲介機関システムで分担管理するアーキテクチャが前提であるため、口座残高型の場合には、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、U T X O 型の場合には、トークンの真正性チェックのた

¹ プレゼンテーション資料の要旨は以下を参照。
https://www.boj.or.jp/paym/digital/d_forum/dfo240816a.pdf

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、セキュリティ耐性は向上する一方、全体としてのスループットやレイテンシーは劣化する可能性等が考えられる。

3. ディスカッション

- 上記プレゼンテーションに関し質疑応答が行われた。概要は以下のとおり。

(参加者) プレゼンテーションではCBDCの性能拡張性への対応の一つとして、データベースの水平分割（シャーディング）が紹介されたが、シャーディングに関し2点質問がある。1点目が、シャーディングにおける分散キーの設定の仕方について、ハッシュベース方式ではキーの順序性が損なわれるとの説明があったが、そのことがどのような問題を生じさせる可能性があるかと考えるか。2点目は、シャードの数と各シャードに格納するレコード数の最適なバランスについて、どのように考えるか。

(プレゼンタ) 1点目については、キーの順序性が損なわれると運用面で複雑性が増すといった程度の問題が生じると考える。2点目については、最適解はわからないものの、シャードの数を増やすと、パフォーマンスは向上するもののコストはよりかかってくるというトレードオフはあるように感じており、データベース設計の際にはこうしたトレードオフを意識する必要があると考える。

(参加者) 2点質問がある。更新処理集中時の対応として、レコード分割を一案として挙げられているが、こうしたレコード分割を施した口座残高型は、UTXO型と整理できるのか。2点目は、UTXO型であっても更新処理集中の際にはレコードロックが必要となり、性能上のボトルネックとなり得るのではないか。

(プレゼンタ) 1点目については、UTXO型をどう定義するか次第ではあるものの、レコード分割は口座残高型における性能上の工夫策の一つと理解しており、レコード分割を施した口座残高型は引き続き口座残高型と考える。2点目については、UTXO型においても更新処理が集中した場合には、後続処理を待機されるレコードロックは必要になると考えるが、トークンの粒度が細かいほど、更新処理の集中自体が起こりづらくなり、レコ

ードロックに伴う処理遅延も発生しにくくなるを考える。

(日本銀行) トークンの粒度の問題というのはその通りと考える。UTXO型と口座残高型は違う概念として論じられることが多いが、口座残高型でも口座を分けたりレコードを分割したりすれば、レコードロックの範囲を限定でき、実態としてUTXO型と同様の並列処理が可能となって、処理集中に伴う性能面での問題が生じにくくなる、という見方もある。

(参加者) 更新処理集中とそれに伴う性能劣化をどの程度回避できるかは、データモデルというより、UTXO型ならトークンの粒度の細かさ、口座残高型ならレコード分割の程度といったように、トランザクションの処理の粒度を最適化する方向で対応できる可能性があるかと理解した。

(参加者) トランザクションの更新処理の観点では、データモデルの違いは、粒度の問題であるという指摘には同意。しかしながら、処理内容やデータベースの構成によっては、データモデルの持つ特徴や性質の違いが生じる可能性がある。

(参加者) データモデルの本質的な違いとして、口座残高型はアカウントに直接紐づく形で残高が管理される仕組みのため匿名性が持ちづらく、UTXO型の場合にはまずアセットがありそれが誰に帰属するかという処理の仕方であることから、アカウントから管理を切り離しやすく匿名性を持ちやすいという傾向がよく言われるが、どう考えるか。

(プレゼンタ) 口座残高型であっても、例えば、台帳のデータベースにはIDしかなく、名前や住所といった情報は仲介機関が管理し、IDのみで送金を行うようにすれば、必要なプライバシー保護は達成できると考える。

(日本銀行) プレゼンテーションに関して2点質問。更新処理集中時の対応策として、出金と入金でトランザクションを分けた上で、入金に関してのみ複数のトランザクションを集約し、更新処理数を減らす案を説明いただいたが、入金と出金のアトミック（一体不可分）性²はどのように担保するのか。もう1点は、仲介機関ネットワークでは、トランザクション保証や取

² トランザクションに含まれるタスクが、全て実行されるか、全く実行されないことを保証する性質を指す。

引電文のルーティングと、処理内容が相対的に多いが、リソースの負担は相応に大きくなる感触か。

(プレゼンタ) アトミック性については、トランザクションを一つに集約した後、被仕向けの仲介機関からの応答がなくリカバリが必要になった場合どうするかなど、検討すべき課題はあると認識している。仲介機関ネットワークでは、この口座であったらこの仲介機関にといったルーティングの情報は持つものの、台帳の更新処理といった重たい業務は行わないため、そこまでリソース負担は大きくない感触。

(日本銀行) トランザクションのアトミック性に関しては、技術的にどこまで厳密に実現することを目指すかという点について、いろいろな意見がありそうだ。技術だけではなく他の仕組みと組み合わせながら、結果的に価値移転がしっかり行われるような方法もあるだろうし、様々なアプローチを柔軟に考えていければと思う。

- 口座残高型とUTXO型のメリットやデメリットに関し、少人数に分かれてのグループディスカッションを行った後、全体でディスカッションを行った。全体ディスカッションの概要は以下の通り。

(参加者) データモデルの比較を行う場合には、前提となるシステムやデータベースの構成を明らかにし、それに基づき議論をする必要があるという点について、グループ内では認識が一致した。

UTXOモデルの特徴として、並行処理がしやすい側面がある一方、例えばスマートコントラクトを適用する際には設計が複雑になる点など、検討事項があるとの意見があった。また台帳が分担管理である場合、UTXOがアンspentであることなどを確認する真正性検証を行う中央システムが必要となり、その負担が重いのではないか、との指摘があった。

(参加者) 同じUTXO型でも、ビットコインと米 Project Hamilton で想定されているものは、大きく違いがあるとの意見が聞かれた。例えば Project Hamilton の場合、中央のシステムは、ハッシュ値のみ管理し、ダブルspendがないことを確認するアーキテクチャになっており、処理が軽くなっている側面もある、との指摘が聞かれた。

(参加者) ユーザーにとって利便性の高いサービスを提供しやすいデータモデ

ルであるかどうか、という観点でデータモデルを評価してもいいのでは、との意見が聞かれた。

(参加者) 口座残高型において口座分割やレコード分割などの工夫を施すことで、UTXO型に優位性があるとされる並列処理が可能となり、ユーザーからすれば両者に本質的な違いはないのではないかと、といった指摘が聞かれた。

(日本銀行) NTT データのプレゼンテーションでは、システム構成などについていくつか前提を置いた上で、口座残高型とUTXO型の比較をしていたが、同じ前提であっても違う解釈ができるのか、前提を変えると違う解釈ができるのか、興味がある。例えば、基本的な設定は揃えた上で、評価をするにあたり必要な追加的な前提を明らかにしながら、データモデル比較がどのように変わっていくか、今後ご意見を伺えればと考えている。

(参加者) 基本的な設定は揃えつつ、異なる観点でデータモデル比較を試みるのは、非常に良いアイデア。例えば、NTT データのプレゼンテーションでは、トークンの検証が行われるUTXO型に比べると、口座残高型はセキュリティリスクへの耐性が想定的に低下するとなっているが、口座残高型であっても中央システムで最初に照合を行う形に変更するなど、工夫次第では評価が変わってくるようにも感じる。

(参加者) システムの前提を置き、それに基づく形でのプレゼンテーションを今回頂けたことで、議論が深まったと感じる。今後も前提を明らかにしながら、目線を合わせた議論ができることに期待している。

(プレゼンタ) 今後ぜひ、他の方のデータモデル比較のプレゼンテーションをお伺いしたい。違う意見もあろうかと思うし、同じ意見となればそれはそれで心強い。

(日本銀行) ご説明いただいたアプローチ以外にも、様々な考え方があると思う。例えば、口座残高型については、トランザクションの集約や、キーバリューベースのNoSQL データベースを用いたシャーディングが提案されていたが、それ以外の方法、例えばレコード分割やNewSQL データベースの活用など、異なるシステム構成を考えることも可能と考えられる。

またUTXO型についても、トークンの生成をどのシステムが行うか、台帳が中央管理である場合に真正性検証を行うかなど、様々なバリエーションが考え得る。

(日本銀行) 口座残高型とUTXO型の優劣をつけることが目的ではなく、データモデルが持つ特性を、前提となるシステム構成や関連する技術とセットで理解していくことが目的であり、こうした試みを通じ初めて、将来的に必要な技術を適切に採択できるのではないかと考える。

(参加者) I o T (Internet of Things) の世界まで考慮すると、マシン同士のやり取りであるM2M(Machine to Machine)が増加し、口座の数が膨大になると考えるが、このような世界までスコープに入れて検討してもよいか。

(日本銀行) 将来的なユースケースとして、様々な可能性を排除せず、検討いただければと考えている。

(日本銀行) 今回は、様々な前提を置いた上で評価軸ごとに評価をいただき非常に議論が深まったと感じる。データモデル比較のプレゼンテーションに関しては、有志の方を対象に調整させていただきつつ、今後も本WGの皆様と解像度を上げていく議論を出来ればありがたい。

4. 次回予定

次回の会合は5月14日(火)に開催。

以 上

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 3 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

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

株式会社 Startale Labs Japan

(事務局)

日本銀行