【新たなテクノロジーとCBDC】WG　第3回会合
CBDCに関する性能面の課題と対応の方向性サマリー

2024年4月10日

（株）NTTデータ　増田　博人

WG4　第3回　NTTD発表内容サマリー（1/3）

1. 背景

中央銀行デジタル通貨に関する実証実験「概念実証フェーズ2」結果報告書に記載されている性能面に関する課題を取り上げ、各課題に対する対応の方向性を示した。具体的には、更新処理集中の緩和策、トランザクション保証の仕組み、DBサーバの水平スケーリング、口座残高型とUTXO型のプロコン分析である。

2. 更新処理集中の緩和策

設計パターン2（口座残高型）では、仲介機関を跨って送金する場合、仕向仲介機関のユーザ口と被仕向仲介機関のユーザ口の更新が必要となり、ユーザ口に更新処理が集中すると待ちが発生し、ボトルネックとなる。これに対して、ユーザ口のレコードを分割することで、分割した数だけ並列処理が可能となり処理集中を緩和できるが、残高合計値が必要な場合には足し上げる処理が必要になったり、処理が偏らないように分割したり、運用中にレコード分割の見直しが必要になるなど、追加の課題が生じる可能性がある。

この課題の対応の方向性として、レコードを分割せずに、複数のトランザクションを1つに集約する（ただし、取引の明細は1件ずつ出力する）ことで更新処理数を削減し、処理集中の影響を大幅に緩和する対策を提案した。

3. トランザクション保証の仕組み

DBの水平分割（複数のサーバ間で整合性のとれた処理の実現）や中央銀行台帳上の口座振替と仲介機関台帳上の口座振替を別々のタイミングで行う（取引のアトミック性の維持）場合には、システム内のトランザクション保証およびCBDCシステム全体（中央システム、仲介機関NW、仲介機関システム）でトランザクションを保証する仕組みが必要である。

特にCBDCシステム全体でトランザクションを保証するためには、仲介機関NWにおいて、トランザクションの処理状況の可視化、業務チェックエラー時の補償トランザクション（ロールバック）の実行、システムエラー時のバックアウトや再実行処理等が必要となる。

WG4　第3回　NTTD発表内容サマリー（2/3）

4. DBサーバの水平スケーリング

性能拡張性においてはDBサーバの水平スケーリングが必要で、シャーディング、分散キー、リバランスの3つを考慮することが重要である。

シャーディングは、大きなDBを複数の小さなパーティション（シャード）に分割し、それぞれのシャードを別々のサーバに格納する分散方式である。分散キーに基づいてトランザクションを各シャードDBに分散することでパフォーマンスを向上し、シャードDBを追加することで水平スケーリングを実現する。このため、分散キーの設計が重要となる。

分散キーの設定には、ハッシュドベースド、レンジベースド、リストベースドがあるが、偏りを少なく分割するにはハッシュドベースドが適している。ただし、キーの順序性が失われるデメリットがある。

システム運用中には、あるシャードにデータが集中しすぎたり、シャードのストレージ容量がひっ迫したりして、性能が劣化することがある。このような場合には、リバランスにより、ワークロードをほかのシャードに分散させることで、データの偏りやストレージ容量の増加の問題を解消する。

5. 口座残高型とUTXO型のプロコン分析

UTXO型は複数のリクエストを並列に処理できるメリットがあることから、口座残高型とのプロコン分析を行った。なお、さまざまな事業者がCBDCエコシステムに参加し多様なサービスを提供するなかで、安全な取引を円滑に行うために、中央システムにおいてトークンの真正性を確認するアーキテクチャとした。

口座残高型では同一仲介機関内の取引は中央システムを介さずに処理できるが、UTXO型ではすべての取引で中央システムによるトークンの真正性チェックを行うため、セキュリティ耐性は向上するが、スループットやレイテンシーが劣化する可能性がある。なお、口座残高型もUTXO型も共通のシステム構成で構築する想定のため、並列処理性は同等である。

WG4　第3回　NTTD発表内容サマリー（3/3）

概念実証で明らかになった性能面の課題等

設計パターン2

仲介機関を跨ぐ移転の負荷量が増えた場合、ユーザ口（ユーザのCBDC残高合計値）に**更新処理が集中し、レコードロックの影響に伴う性能劣化が生じる**可能性がある。

仲介機関のユーザ口のレコード分割（**残高を求める場合に合算処理**が必要）

中央銀行台帳上の口座振替と仲介機関台帳上の口座振替を別々のタイミングで行う（**取引のアトミック性の維持**が必要）

性能拡張性

DBサーバ：**水平分割**（シャーディング）により、各シャードのデータ量やアクセス量を抑制し、処理性能を確保する。

複数の**サーバ間で整合性のとれた処理**の実現

データ量やアクセス量に**偏りがでないよう、定期的なチューニング**が必要

変動額面方式のトークン型台帳
（UTXOモデルに類似したデータモデル）

複数のリクエストを並列に処理できる。

口座型と比較した場合、必要な**リソース使用量が増える**可能性や性能を維持した形での保有額制限といった**周辺機能の実装の難度が上がる**可能性がある

対応の方向性

1. 口座に対する更新処理数を削減することで、処理集中の影響を緩和
2. システム内でトランザクションを保証する仕組み

   CBDCシステム全体でトランザクションを保証する仕組み
3. DBサーバの水平スケーリングの留意点（シャーディング、分散キー、リバランス、課題）
4. 中央システムでトークンの真正性を確認するアーキテクチャを前提として、口座残高型とUTXO型のプロコン分析

出典：中央銀行デジタル通貨に関する実証実験「概念実証フェーズ2」結果報告書


NTT DATA