

2025年3月25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6回会合の議事概要

1. 開催要領

(日時) 2024年9月12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

- ソラミツ株式会社より、「口座型、UTXO型データモデルの比較」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。
 - ・ 分担管理型の台帳システム構成などの前提²を置き、①口座型、②口座型withDLT、③UTXO型のデータモデルを比較。
 - ・ ①と③は第3回会合でNTTデータが提示したのと同じモデルであり、②のモデルが、今回新たに検討したもの。
 - ・ ②の場合、取引処理を行う仲介機関の台帳システムには、DLTを活用する一方、自己口及びユーザ口等を管理する中央システムについては、取引履歴のみDLTを活用し、残高情報管理は通常のDBで行うハイブリッドなアーキテクチャを想定することで、性能を大きく落とさず、二重払いや改ざん防止といったセキュリティ耐性を向上できる可能性を指摘。

¹ 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/df0250325a.pdf

² 分担管理型の台帳システム構成は、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を指す。その他の前提条件は次の通り：送金機能を対象に、各種制限（ユーザー単位で、保有額や取引額および取引回数を制限）を課し、性能要件は「通常スループット数万件/秒、ピーク時スループット10万件以上/秒、レイテンシー数秒以内」とする。

- 大和証券株式会社・野村証券株式会社より、「CBDCを用いた有価証券の決済」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。
 - ・ セキュリティトークン（ST）は、株式・社債・受益証券発行信託等の有価証券をブロックチェーン上にトークンとして発行したもので、トークンの移転と権利の移転が一体となっているものと言われている。国内で発行されているSTは、主に不動産、社債の2種類で、現時点の発行額の規模としては不動産STの方が大きい。また、社債STではグリーン・デジタル・トラックボンドという新しい商品が登場している。
 - ・ STのメリットは、ブロックチェーンが受益権原簿となり、その上で投資家情報をリアルタイムに管理することで、従来、信託銀行が管理する際に対応が困難であった公募形式・小口での発行ができることのほか、投資家への利得付与（ユーティリティトークン）を行うマーケティングに活用できることや、将来的には、スマートコントラクトによる商品ラインナップの拡充やポストトレード業務に係るコスト削減効果などが期待されている。
 - ・ ST市場の拡大にあたっては、決済リスクの低減やクロスチェーンへの対応などが課題。決済リスクの低減を実現させるための選択肢の一つとしては、CBDCを用いたDVP決済が挙げられ、例えば以下のようなスキームが考えられる。
 - ✓ リテール型：取引所での取引約定後、証券会社のシステムを介してST基盤へ決済指図を伝達。売り手と買い手である顧客間の資金・ST決済は、市中銀行にそれぞれ開設したCBDC口座を通じて、ST基盤間とデータ連携しながら、リアルタイムのグロス決済を行う。
 - ✓ ホールセール型：取引所での取引約定後、証券会社のシステムを介してST基盤へ決済指図を伝達。取り扱い証券会社間の資金・ST決済のうち、ST決済は、ST基盤上で証券会社ごとのオムニバス口座に取引内容を集約し、証券会社間でネッティングされ、資金決済は、CBDC基盤には証券会社が保有する口座を通じて、ST基盤とデータ連携しながら、時点ネット決済を行う。

3. ディスカッション

- 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、以下のとおり。

(参加者) DLTの耐改ざん性を担保する肝は、相互検証によって生まれているという認識であるが、口座型 with DLTにおいては、中央システムという一つの主体が複数のノードを持つアーキテクチャは、DLTの良さが引き出されない実装なのではないか。

(プレゼンタ) ご指摘の通りで、複数の金融機関がコンソーシアム的にノードを持ち合うことが理想。ただ、高い性能要件を満たすために、中央システムによる残高管理とは切り離し、取引履歴の耐改ざん性を保証するために非同期で取引履歴だけDLTに保存する形にしている。

(参加者) 複数主体ではなく、単一主体が保有する複数ノードで構成されるDLTであっても、単一主体が単一データベースを保有することに比べて耐改ざん性や真正性の担保が向上するという理解でよろしいか。

(プレゼンタ) ご理解の通り。単一主体であっても、複数のノードとして、複数のデータベースを例えば地理的にも分散させて運用することで、各ノード間での相互検証・監視が行われる形となるため、セキュリティを向上できると考える。

(参加者) 口座型 with DLTの性能評価について、中央システムの残高更新処理ではなく、仲介機関システムの取引処理を対象にした場合には、性能は低下する可能性はあるか。

(プレゼンタ) ご指摘の通り。評価対象をどこに設定するかで、性能の評価は変化するだろう。

(参加者) 各種制限判定のうち、例えば保有額制限判定で必要となる残高確認について、厳密性を求めると中央システムでの対応が必要であるが、例えば簡易的にエンドポイント(ウォレット)で対応する形とすれば、UTXO型であっても性能を大きく落とさず対応が可能となるのではないか。

(プレゼンタ) ご認識の通り。保有額制限判定を即時ではなく日次で行うこと

でウォレットでの対応も可能となり得るなど、どの程度厳密性を求めるかでも、性能面の評価は変化し得る。

(参加者) U T X O型に関して、各種制限をユーザー単位で厳密にかけようとすると性能への影響が非常に大きく、実装はできるものの追加コストによって実装ハードルが高くなっている認識。

(参加者) 口座型 with D L Tの中央システムでは、残高更新を行う中央集権型DBと、取引履歴を管理するD L Tが非同期という前提となっているが、中央集権型DBとD L Tの間で不整合が発生した場合の検証・更正処理はリアルタイムで行われるのか、バッチ処理を想定されているか。

また、セキュリティを考える上でどのような脅威モデルが想定されているのか。

(プレゼンタ) 不整合の検知タイミングは現状未検討でご指摘の通り、リアルタイムもしくはバッチ処理での対応の必要がある。D L Tに記録されたデータの改ざんは困難であるためD L Tに記録された内容を基に更正を行うものとする。

脅威モデルについては、内部犯行や内部の作業ミス、外部からのハッキング等様々な可能性が考え得る。

- 大和証券株式会社と野村証券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、以下のとおり。

(参加者) ブロックチェーンを利用する際のスケーラビリティの課題についてはどうお考えか。例えば、株式など高頻度な取引に関してS T化は難しくなるか。また、S T化のメリットの一つとして説明されたスマートコントラクト活用について具体例はあるか。

(プレゼンタ) ご指摘の通り、取引の頻度が高い商品のS T化はスケーラビリティの課題がある。ただ、例えば、現時点でS Tの販売額の多くを占める不動産は、中長期の保有を前提としているため、そうした課題はあまり発生していない認識。

(参加者) スマートコントラクトの活用に関しては、複雑な金融商品への応用

可能性があると考え。例えばサステナビリティリンクボンドといったKPIの達成状況に利払いが連動する商品の場合、条件に応じた利払いを手動で対応すると煩雑でありスマートコントラクトの業務効率化の恩恵を享受できると考える。

上記とも関連するが、STの将来を展望すると、個別のニーズに対応する形で複雑なロジックをスマートコントラクトで実装するとなると、そのような商品の決済件数はあまり大きくはならず、現時点ではスケーラビリティの課題は大きな論点にはならない印象。

(参加者) スマートコントラクトの活用例として、海外事例では、BlackRockがBUIDLというマネーマーケットファンドをトークン化し、スマートコントラクトで利払いを行っている。

(参加者) 不動産STや社債STといったアセット側のトークン化は進展しているが、それらの決済は、現状、従来通り民間銀行預金を利用している認識。STの決済において、今後、CBDCやステーブルコインといったデジタル通貨を使ったDVP決済の将来像はどの程度描かれているのか。

(プレゼンタ) 民間デジタル通貨を利用したDVP決済の机上検証は行っているが、実用化には至っていない。実用化に際しては証券会社のシステム対応といった課題も想定される。

またデジタル通貨の導入によって仮にT+0が実現すると、取りはぐれリスクは解消する一方、プレファンドの負担が増加し、資金効率が低下する側面には留意する必要がある。

(参加者) ST決済について、市場の安定性や決済の効率性の観点から、一定の過渡期には民間デジタル通貨での決済はあり得るが、最終的には安定性が最も高い中銀マネーであるCBDCでDVP決済を行う方向性が望ましいと考える。

(プレゼンタ) ご指摘の通りと考える。ただし、現在においても、STの決済は民間銀行預金を利用されおり、中銀マネーか民間マネーで決済するかは、ユースケースに応じた使い分けを考えていく必要がある。なお、例えば、適切なレギュレーションで、かつ価値変動が円と連動している前提であれば、ステーブルコインをSTの決済に利用できる可能性はある。

- (参加者) リテール型CBDCを活用したST決済について、売り手と買い手である顧客のCBDC口座は各市中銀行に存在しているため、ST基盤とのデータ連携において工夫をしないと、煩雑な接続になる可能性はあるか。
- (プレゼンタ) ご指摘の通り。CBDCシステムに対して単一の接続先が存在し、データ連携が可能となる仕組みが実装されることが好ましいかもしれない。
- (参加者) ST決済において避けたいケースとしては、約定後に決済が履行されないことが挙げられる。決済完了まで資金をロックする対応などが考えられるが、注文の変更がある都度ロック・アンロックをすると、スケーラビリティの課題も含めて実装ハードルが高い可能性がある。
- (参加者) 海外では、日中流動性を確保するためのユースケースとして、株を担保に資金調達を行うユースケースもあるが、今後STのアセットクラスの拡充はどのようなものが見込まれるか。
- (プレゼンタ) 例えば美術品など、これまで投資機会を十分に提供できていなかったアセットのトークン化が考えられるが、法的なハードルもあり現状アイデアベースにとどまっている。
- (日本銀行) アセット側の進展によって資金側に求められる機能も変化し得る点は、示唆的である。そういった中で公的機関、民間事業者が社会全体として好ましい方向に進んでいけるように資金側の進展をどのように対応していくかが重要であると感じた。
アセット側の進展のご意見をいただいたが、同様の観点でトークン化資産の発行・流通プラットフォーム基盤の将来性について海外との比較も交えてお伺いしたい。
- (参加者) プラットフォーム基盤について考える際には、プライベート・コンソーシアム型ブロックチェーンなのか、パブリックブロックチェーンであるかで区別される。パブリックブロックチェーンであれば、グローバルで繋がるのが可能であり、また決済手段としてステーブルコインが利用できるメリットがある。海外では、一部でパブリックブロックチェーンが利用されているが、日本では、規制の関係上プライベート・コンソーシアム

型ブロックチェーンが利用されている。今後の課題は、如何に決済手段との相互運用性を実現していくかがあると考える。

(参加者) チェーン間を繋ぐ相互運用性の技術に関しては、繋ぐ部分（ブリッジ）の脆弱性にどう対応していくかといった観点で、様々な方法論がありデファクトは決まっておらず、標準化の議論もこれからである。こうした下で、現状、ユーザーからの対応ニーズが大きいパブリックブロックチェーンでのユースケースが先行しているため、今後の会合でいくつかご紹介したい。

(日本銀行) データモデル比較のプレゼンテーションでは、口座型 with DLT という新しい組合せを紹介いただき非常に参考になった。STの議論では、技術の進展と制度設計は両輪であり、バランスが取れて初めて新しいサービスが生まれると感じた。今後も本WGを通じて議論を深めていきたい。

4. 次回予定

次回の会合は11月1日（金）に開催。

以 上

CBDCフォーラム WG4
「新たなテクノロジーとCBDC」
第6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

TIS 株式会社

(事務局)

日本銀行