2024 年 11 月 1 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４回会合の議事概要

１．開催要領

（日時）2024 年５月 14 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

- 株式会社 Startale Labs Japan より、「ブロックチェーンを使用したＣＢＤＣの可能性に関して」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]。

  ・ 加速する技術革新の中では、これまでの当たり前を前提とせず 20～30 年後も視野に入れて検討することに意味がある。思考実験としてパブリックブロックチェーン上にＣＢＤＣが発行される世界を考えると、以下のような論点・課題が存在する。

  ✓ スケーラビリティ：通常のデータベースと比べると、例えばEthereumでは分散性やセキュリティを重視する分、スケーラビリティが劣る点で課題があるが、一部処理をバッチ化する別のチェーン（レイヤー２）の作成により、処理性能を上げる技術も出始めている。もっとも、高いスループットを出すと言われているチェーンであっても、そこで言われている性能値は実験環境における理論値であることが多く、実測値はサーバーの立地や取引量等により理論値より低くなっているケースが多い。

  ✓ プライバシー：ブロックチェーンでは全ての取引情報が公開されプライバシーが守られないと認識されがちだが、ゼロ知識証明を用いることで、データの秘匿性を保ちながら取引の正当性を参加者全員

[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/dfo241101a.pdf

で合意することが可能となってきている。

- ✓ セキュリティ・障害耐性：ブロックチェーンは改ざんが極めて困難な仕組みであるものの、バリデータが少ない際の分散性の低さやスマートコントラクトの脆弱性に対する攻撃といった危険性がある。またチェーン内外を繋ぐブリッジの脆弱性を標的にする脅威も課題である。
- ✓ ガバナンス：パブリックブロックチェーンはハードフォークの可能性があるため、オフチェーンでのガバナンスも使うことで、望ましい体制を検討していく必要がある。
- ✓ ユーザーエクスペリエンス・インターオペラビリティ：ウォレットの作成や秘密鍵の管理等について、現状のブロックチェーンはＵＸが良くないが、Account Abstraction や Chain Abstraction といったＵＸ向上技術が登場している。クロスチェーンブリッジやアトミックスワップなどの技術により、他のブロックチェーンやデジタル通貨との相互運用性も向上し得る。

・ 上記論点・課題を踏まえると、パブリックブロックチェーン上でのＣＢＤＣの発行は、現時点では、特にスケーラビリティの観点で、ハードルが高い。

・ そのため、ＣＢＤＣをブロックチェーン上で取り扱う方法としては、民間事業者が保有するＣＢＤＣを裏付け資産としてロックし、その民間事業者がパブリックブロックチェーン上で wrapped ＣＢＤＣの形で発行・流通させる方法が一つの選択肢となる。wrapped ＣＢＤＣの移転に関しては、ＡＭＬ／ＣＦＴの観点から、例えば、特定のウォレットやスマートコントラクトのみ利用可能なホワイトリスト設定を行うなど、一定程度の制御をかけていくことも可能。

・ 上記のような方法でＣＢＤＣを裏付け資産とした wrapped ＣＢＤＣがパブリックブロックチェーンに流通した場合には、新しい経済活動のユースケースが生まれ、トークン経済が発展する可能性が期待される。

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。

（参加者）性能拡張の手段として別のチェーン（レイヤー２）を作成し、レイヤー２で複数のトランザクションを一つにまとめてバッチ処理し、その結果をレイヤー１に報告しファイナライズする技術について紹介いただいた。具体的なバッチ化の手法としては、①オプティミスティックロールアップ（レイヤー２での処理を正しいと仮定し、一定期間、処理結果の不正証明を申し立てるチャレンジ期間を設け、不正が証明された場合には処理の取り消しができる）と、②ＺＫロールアップ（レイヤー２でのバッチ処理の時点で、不正がないことも同時にゼロ知識証明で証明し、レイヤー１に報告）について、ご説明いただいた。

プレゼンテーションでは、①と②のスループットの理論値について、後者の方が高いと紹介されていたが、実測値はどうであるか。

（プレゼンタ）実測値では、ＺＫロールアップのスループットは、オプティミスティックロールアップより出ていない感触。ＺＫロールアップは開発が難しく、オプティミスティックロールアップは開発者フレンドリーで Ethereum とほぼ同じ環境で実装できるため、現在は、オプティミスティックロールアップの方が主流となっている。

（参加者）プレゼンテーションでご紹介のあった各チェーンの性能値については、一部チェーンについては数万 TPS 出ると言われているものもあるなか、実測値としては総じて数十～数百 TPS 程度しか出ておらず、理論値と実測値の乖離がかなり大きい点は、示唆的である。理論値は、あくまで性能測定において理想的な実験環境下のものであるという点を認識しつつ、現状の低い実測値のみで判断するのではなく、将来の技術革新の可能性も踏まえ、新しい技術の進展をみていくことが重要と考える。

（プレゼンタ）ご指摘の通り。例えば生成ＡＩの場合、ハードウェアの進展が大きく影響していたように、関係ないと思われていたイノベーションが思わぬところで異なる技術革新に繋がるケースは多い。技術の進展は、他の関連する技術とセットでみていく必要がある。

（参加者）プライバシー保護の課題に関連して、ＣＢＤＣというユースケースを考えたときに、プライバシーが完全に保護されるとＡＭＬ／ＣＦＴへの対応が困難になるという関係性があり、そのバランスの取り方について明確になると、さらに良い議論になるのではと考える。

（プレゼンタ）ご指摘の通りで、適切なバランスについてはまだ見えていないが、特に一般利用型ＣＢＤＣを検討する場合には、個人情報がどのように取り扱われるかは非常にセンシティブであると理解している。

（参加者）プライバシー保護と透明性のバランスは、各国の事情に応じ、ゼロ知識証明のような技術でもってきめ細かく調整可能にしながら、検討していくことが重要であると考える。

（参加者）分散性・スケーラビリティ・セキュリティにトレードオフが存在するという、ブロックチェーンのトリレンマを踏まえると、今回ご説明のあった、スケーラビリティを向上させる取り組みに関しては、分散性を犠牲にしていると解釈することができると考えるが、いかがか。

（プレゼンタ）ご認識の通り、現時点においてはトリレンマの中だと分散性が犠牲になることが多い。参加者を特定したコンソーシアムブロックチェーンも、ある種の分散性を犠牲にスケーラビリティを向上させている一例だと考える。

（参加者）オプティミスティックロールアップについて、実際に不正が発覚したケースはどれくらいあるかお伺いしたい。

（プレゼンタ）過去に数件あったか程度で、あまりない認識。不正防止ができるように開発元がアライアンスを組んで有償でモニタリングしていることもあり、不正自体があまり発生していないと考えている。

（参加者）不正検知の仕組みは、将来的にはＺＫロールアップのような技術を使って取引証明をするものがいいと感じる一方で、オプティミスティックロールアップのように誰かが監視する方法もやはり残っていく可能性もある。後者においては、インセンティブ設計といった動機づけが一つのポイントになると考える。

（参加者）スケーラビリティに関してはスループットの話が中心であったが、ユーザーの利便性を考慮すると、レイテンシーに関しても追加的な論点となり得る。

（プレゼンタ）レイテンシーに関しては、どの時点でファイナルと見做して計

測していくかといった観点で検討していく必要があると考える。ブロックチェーンではブロックの生成速度がレイテンシーに大きく影響するため、ブロックの生成速度を速くすることで低レイテンシーが実現できるが、スマートコントラクトなどの柔軟性は損なわれるというトレードオフは存在する。こうしたトレードオフを踏まえた上で、ユースケースに応じてどの程度のレイテンシーを求めるかは、包括的に議論していく必要がある。

（参加者）パブリックブロックチェーン上でのＣＢＤＣの発行について、思考実験としてある種割り切りながら、主要論点に関し評価をしていただいたことと認識。スケーラビリティに関しては、数十年スパンでみた場合には技術が進展する可能性もある。wrapped ＣＢＤＣのご提案は、ＣＢＤＣの発行は中銀が行う一方で、wrapped ＣＢＤＣの流通はパブリックブロックチェーン上で行われる形で、機能がアンバンドルされている理解であり、そうした中で、中央銀行をはじめとした公的機関の役割はどのようなものなのか、考えていきたい。

（プレゼンタ）パブリックブロックチェーンが全てをリプレイスするとは考えていない。既存のサービスの中では、中央集権的に進めた方が効率的なものの方が多い。分散化すべきところとそうでないところの使い分けが重要と考えている。例えば、オンチェーンで成立した取引が不正なものであった際に、リアルな世界での法的な擦り合わせや解消を行う役割は必要であり、そういった領域に公的機関の役割があるのではないか。

（プレゼンタ）プレゼンテーションでは、国際送金に関して、ＣＢＤＣがコルレス銀行を介さずブロックチェーンで流通することで、効率化できる可能性について言及したが、さらに妄想での話として、DeFi の世界において、例えば、日本円や米ドルＣＢＤＣをラップ化した資産で流動性を提供したユーザーに手数料収入が入る仕組みができると、新しい需要が創出される可能性もあるかもしれない。

（参加者）国際送金にＣＢＤＣを用いることは、ジャストアイデアとしてご紹介いただいたが、そうしたコンセプトで実験を進める例も、海外では実際にでてきている。一般利用型ＣＢＤＣの議論において国際送金はメインの対象にはならないものの、本ＷＧにおいては、そういった制約をあまり意識せず、想像力を働かせながら将来の話を議論できればと考える。

とはいえ、DeFi のような世界まで展望した場合、中央銀行マネーがどの

ようなユースケースまで利用することが許容できるかは、今後議論が必要と考える。wrapped ＣＢＤＣになった時点で正確には中央銀行マネーではなく、民間の自由に任せるという見方もあるかもしれない。

（参加者）wrapped ＣＢＤＣの発行体をどのエンティティとするか、また、ご紹介のあったホワイトリスト登録などで流通の範囲を制限するかしないか、するとしたらどの程度にするかなど、実装においては、様々なオプションが考えられるだろう。

（参加者）各国中銀とＣＢＤＣについて会話する中で感じたのは、ブロックチェーンを活用するにあたり、発行量のコントロールをはじめ、何らか中央集権的なガバナンスの役割を果たしていきたい意向が多い。一方、国際送金のユースケースの場合には、ガバナンスをどの国がとっていくのかが議論になりやすく、各国の間に入る形で、パブリックブロックチェーンが活用されやすい可能性があるのではないか。

（プレゼンタ）ＣＢＤＣが、国際送金などの特定のユースケースで利用する姿を検討するのであれば、パブリックではないブロックチェーンで発行・流通する方が良いと考える一方、特定のユースケースを定めず、DeFi など様々な技術との掛け合わせで、新しいものを生み出す可能性も視野に入れる場合には、パブリックブロックチェーン上で流通していく姿も考えてみてもよいのかもしれない。

（参加者）ＣＢＤＣの使途に関しては様々な考え方がある。例えば、銀行券は、紙幣であるという技術的な結果として、使途によらず使用可能であり、かつ匿名性を持つ形になっているが、ＣＢＤＣにも銀行券と同じ機能を持たせるかという観点でも議論がある。wrapped ＣＢＤＣのアイデアは、価値の裏付けとしてＣＢＤＣを使いながらも、パブリックブロックチェーン上で流通し使途の柔軟性を持つ、一つの興味深いアイデアだと考える。

（参加者）wrapped ＣＢＤＣを流通させる際は、カストディーの信頼性をどう確保していくか、利用者のデジタルリテラシーの問題にどのように対応していくか、について検討していく必要性を感じる。

（参加者）DeFi などの Web3 的世界が仮に大きくなった際に、ＣＢＤＣのよう

な中央銀行マネーがやはり必要となってくるのか、あるいはステーブルコインのような民間マネーでも問題ないのか、ご意見を伺いたい。

（プレゼンタ）例えば、DeFi プロトコルで資金が盗まれたときの補償など、保険会社が Web3 上でサービスを展開した場合、保険金の支払いは、一般的なステーブルコインよりも wrapped ＣＢＤＣが使えれば、大手保険会社も参入しやすくなるのでないかと考える。企業がパブリックブロックチェーンの活用を検討する際には、決済手段として信頼度の高い中央銀行マネーのニーズは根強くあり、wrapped ＣＢＤＣの存在が Web3 的世界における新しいチャレンジを誘引し、より良いユースケース創出につながっていくと考える。

（参加者）銀行券をはじめとする中央銀行マネーは、様々な形で民間マネーと共存しながら利用されている。今後、Web3 的世界が拡大していき且つ重要になった場合、その中で中央銀行マネーが果たす役割は論点になり得ると考える。

（日本銀行）一般的に論じられるブロックチェーンのデメリット、例えばスケーラビリティやプライバシーの課題については、技術的に様々な工夫の取り組みが生まれていることが理解できた。今後も本ＷＧでは、空間的にも時間的にも幅広い世界観で、議論を続けていきたい。

４．次回予定

次回の会合は７月４日（木）に開催。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ４
「新たなテクノロジーとＣＢＤＣ」
第４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 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