

C B D C フォーラム D G 2
「新たなテクノロジーに関するディスカッショングループ」
第 3 回会合の議事概要

1. 開催要領

(日時) 2026 年 9 月 29 日 (火) 14 時 30 分～16 時 30 分

(形式) W e b 会議形式

2. プレゼンテーション

- 株式会社 Datachain より、「オンチェーン金融におけるプライバシー」についてプレゼンテーション¹が行われた。概要は以下の通り。
 - ・ 通常の商取引において、取引内容の開示は関係者に限定する必要があるため、パブリックチェーンを用いたデジタル通貨を運用するうえでは、プライバシー保護が重要な論点となる。この点、法人利用を想定したプライバシー保護技術について、新興のチェーンではプライバシーを確保する機能の標準装備化が進んでいるほか、既存チェーンでもプライバシー実装の動きが急速にみられる。
 - ・ 適切な統制がなされないまま情報が秘匿されると、実態が把握できないほか、問題発生時の対応が全面遮断（コントラクト単位で遮断）とならざるを得ないため、意図しない形で無関係な利用者まで巻き込まれる懸念がある。こうした懸念は、ユースケースの拡大を阻害する要因となることから、監督責任を負う発行体等の事業者が適切な統制機能を持つことが必要である。
 - ・ プライバシーは、匿名性・機密性・非リンク性の 3 要素で構成され、法人利用では、すべてを満たすことが望ましい。なお、オンチェーン金融において求められるプライバシーとは、「完全秘匿化」ではなく、適切な対象に対して必要な情報を開示することができる「選択的開示」。
 - ・ プライバシー技術における秘匿方式は、秘匿環境型・暗号化残高型・選択的データ配布型の 3 つに分類できる。いずれの秘匿方式も、暗号技術が共通の前提となっているが、台帳記録内容の正しさと秘匿を実現するために追加的にどのような信頼を前提としているかという点ではそれぞれ異なる。

¹ プレゼンテーション資料は以下参照。

https://www.boj.or.jp/paym/digital/d_forum/dg2/dfodg261019c.pdf

- ・ 法人顧客に対してプライバシーにかかるソリューションを提供する際には、上記の点を俯瞰しつつ、コンプライアンスが確保できる基盤を開発・提案することでユースケースの拡大に努めている。
- 株式会社 Datachain のプレゼンテーションを受けて、質疑応答が行われた。概要は以下の通り。

(参加者)

- ・ ブロックチェーンに関する一般的なトリレンマとして、スケーラビリティ、分散性、セキュリティが知られている。プライバシー技術を開発するうえで、これらトリレンマとの関係について、これまで議論された点や課題とされている点はあるか。

(プレゼンター)

- ・ ブロックチェーンにおけるプライバシー保護の一手法として、プライベートチェーンやコンソーシアムチェーンの利用が議論されてきた。ただし、これは参加者を限定することで、分散性や、特定の運営者に依存しない改ざん耐性を一定程度犠牲にするものであり、ユースケースによっては望ましくない。ゼロ知識証明等の技術の成熟により、こうした犠牲を払わずに、パブリックチェーン上でプライバシー保護を実現することも可能になりつつある。この意味で、プライバシー保護技術の発展は、プライバシーと分散性・セキュリティとの両立を可能にしつつあると言える。
- 株式会社 BOOSTRY より、「日本におけるオンチェーン金融の動向」についてプレゼンテーション²が行われた。概要は以下の通り。
 - ・ 海外のセキュリティ・トークン（以下、ST）市場は、スタートアップ金融中心にプロ投資家向けに拡大してきた。一方、国内では、大手証券会社や信託銀行を中心に、個人投資家向け市場が拡大してきた。2026 年には、国内公募 ST の累積発行総額が 4,000 億円を突破しており、市場の成熟と多様化が進んでいる。今後の国内市場拡大の方向性として、地域金融機関の参入に加え、大手事業会社による自己募集といった「超直接金融」の発展を期待。
 - ・ グローバル化の観点では、当社は国内 ST を海外に販売するための基盤構築や高度化を展開している。具体的には、国内 ST を海外投資家に販売することを

² プレゼンテーション資料は以下参照。

https://www.boj.or.jp/paym/digital/d_forum/dg2/dfodg261019b.pdf

眺めて、国内およびシンガポールの証券会社と共同で、パブリックチェーンを用いた実証取引を完了。パブリックチェーンである Ethereum と、コンソーシアム型ブロックチェーンの ibet for Fin をミラーリングしながらトークン管理する仕組みを実現。

- ・ ホールセール取引の高度化について、商品ごとに様々なスキームが検討されている。振替口座簿連携案については、既存証券をオンチェーン化で流動化させる取り組みを実証実験している。また、トークン化株式における特定受益証券発行信託案や、トークン化 MMF の非ほふり型の投信スキームの検討が進められている。
 - ・ ST 市場の更なる発展に必要な要素はオンチェーンの資金決済手段。例えば、ステーブルコインが必要だが、コインの不正流出やマネーロンダリングへの対応が課題。この点、パブリックチェーンを用いる場合でも L2 で統制能力を強化する「半パブリック」と言えるような実装も登場している。
- 株式会社 BOOSTRY のプレゼンテーションを受けて、質疑応答が行われた。概要は以下の通り。

（参加者）

- ・ 海外投資家向け ST 販売の実証取引において、パブリックチェーンのみでトークンを管理するのではなくミラーリング方式を採用した背景と、ミラー先がパブリックチェーンなのかプライベートチェーンなのかについて伺いたい。

（プレゼンター）

- ・ 実証取引におけるミラーリングの仕組みは、パーミッション型の ibet for Fin 上で国内投資家向けに発行されているトークンを Lock³し、パブリックチェーン上に Mint⁴する方式。パブリックチェーン上のトークン移転データを常に監視し、それを ibet for Fin 上にトレースして管理することで同期を実現。ミラーリングとした理由は2点あり、①万一パブリックチェーンが停止しても、ibet for Fin 側で権利を保持できる点や、②一連の取引処理が終わればパブリックチェーン上のトークンを Burn⁵し ibet for Fin 上のトークンだけを残すことができるようにすることでパブリックチェーンにかかる様々なリスクを局所化できる点が挙げられる。

³ Lock とは、デジタル資産を一定期間移転できないように固定する仕組み。

⁴ Mint とは、新しいデジタル資産をブロックチェーン上に新しく発行・生成するプロセス。

⁵ Burn とは、ブロックチェーン上のデジタル資産を消滅させるプロセス。

(参加者)

- ・ ST について、日本では大手金融機関が個人投資家をターゲットとしてきたのに対し、海外ではスタートアップ金融がプロ投資家をターゲットにしてきたと説明されていたが、日本と海外で違いが生まれた背景について見解を教えてください。

(プレゼンター)

- ・ 日本において大手金融機関が ST 市場を主導することになった背景としては、法規制の影響が考えられる。ST は、2020 年の改正金融商品取引法で初めて明確に定義され、この法整備を契機に大手証券や大手信託銀行が参入を進め、市場が徐々に成長した。もっとも、スタートアップ金融にとっては規制対応など参入障壁が高く、大手主導で市場が形成されたとみている。一方、海外では規制が先行せず、暗号資産の延長として ST の市場が形成された。このため、スタートアップ金融が参入しやすい一方、規制が未整備であるが故に大手金融機関の参入が難しい状況であったと考えられる。

3. ディスカッション

- ブロックチェーンの今後を題材に、オープン性（透明性・接続性）とプライバシー（セキュリティ・規制適合性）の両立に関するディスカッション⁶を実施した。概要は以下の通り。

(参加者)

- ・ オンチェーン金融は、達観してみれば、決済領域における伝統的金融機関とノンバンクとの競争という見方が可能。
- ・ オンチェーン金融において、パブリックチェーンは顧客利便性を向上させる可能性が高い一方、伝統的金融における規制対応などコンプライアンスとの親和性は低い。プライベートチェーンは、顧客利便性の改善に資するか不透明である一方、伝統的金融に求められるコンプライアンスとの親和性が高い。チェーンの選択において、顧客利便性とコンプライアンスとの親和性を両立させることが課題となる。
- ・ パブリックチェーンは利用者主権型であり、透明性が重視されている。プライバシー技術が開発されたとしても、利用者主権型が出発点だと、金融機関

⁶ ディスカッション資料は以下参照。

https://www.boj.or.jp/paym/digital/d_forum/dg2/dfodg261019a.pdf

が遵守すべき規制への対応ニーズを完全に満たすことが難しいこともあるだろう。このため、プライベートチェーンを起点としつつ、透明性と規制対応のトレードオフに折り合いがつくハイブリッドモデルが伝統的な金融機関にとって望ましいブロックチェーンモデルになるだろう。

(参加者)

- ・ パブリックチェーンを活用する金融機関には、自らの取引内容を秘匿したいという要求がある一方、取引の相手方から受け取る資産が正当な取引を経たものであることを確認したいという要求も抱えており、両者は衝突する。また、資金洗浄者の資金を善意で取得してしまった投資家の資産は、受け取ることに受け取らないことにも問題が生じ得る。このような問題は現金取引では通常生じ得ないものである。
- ・ 規制が有効に機能しつつ、規制遵守に伴うコストを抑え、プライバシーを保護することを同時に達成することは容易ではない。この課題は、私が米国で所属していた研究グループでは「コンプライアンスのトリレンマ」と表現されている。この課題の対応策としては大きく、①参加者を限定する方法（ホワイトリスト管理、プライベートチェーン等）、②審査を通過した人に証明書（Soulbound Token、VC<Verifiable Credential>等）を付与する方法、③自身が有資格者であることのみを証明する方法（ゼロ知識証明技術等）、が挙げられる。①は、プラットフォーム内の管理は容易だが、プラットフォーム外の参加者と接続する際にどのように確認するかという課題が残る。また②も現状、プラットフォームを跨いで証明書を活用できるユースケースは自分の知る限り見当たらない。そうした中、③が近年注目を集めている。
- ・ こうした技術的対応策が登場してはいるものの、依然普及していない背景については、以下2点挙げられる。1点目は、誰が証明を行うのか、また、その行為がビジネスとして成り立つのかが明確になっていない点である。2点目は、正当性の証明を厳密に追及すると、正当性を証明できる特定の集団内でしか取引ができず、結果としてマネーが持つファンジブルな性質が失われる点である。こうした問題に対して、どのようなポリシーを採用するのか決定していく必要がある。

(参加者)

- ・ 金融機関としてデジタルアセットに取り組む大義は、顧客利便性の向上と、リスクマネー供給に資することの2点。
- ・ プライバシーが適切に保護され、かつネットワーク効果のあるブロックチェーンであれば顧客利便性向上への寄与は大きい。ブロックチェーン技術を活用する代表的な利点であるクロスボーダー取引決済の即時性については、特にホールセール顧客のニーズを期待しているが、プライバシーが流出するこ

とは避けなければならない。パブリックチェーンはネットワーク効果が魅力だが、以前はプライバシー保護を兼ね備えたチェーンが見当たらなかった。もっとも、最近の米国等の動向をみていると、一定程度これらのニーズを両立したチェーンが出始めている。

- ・ リスクマネーの供給の観点では、与信行為は資金回収というプロセスを伴うため、取引相手の顔が見えていることが前提。与信取引のこうした考え方と、プリミティブな Ethereum 等のパブリックチェーンが前提とするゼロトラストの考え方は根本的に異なり、相性は悪い。

（参加者）

- ・ 金融グレードのチェーンとして、Canton Network や Arc、Tempo 等が海外で注目が集まっている。全ての情報を秘匿するのではなく、必要な人に必要なタイミングで必要な情報のみを開示できる点が特長である。
- ・ Canton Network では Daml と呼ばれる独自言語を用いてスマートコントラクト等を構築する。ビジネスロジックに従い構築できるので、不用意な事故や不正取引を防止できる点が魅力。一方、独自言語を用いる点などは、技術面や構築面でハードルとなる。
- ・ 金融機関に要求される統制の機能や、セキュリティの仕組みを構築していく際に、業界内で共通の仕組みを育てることができると、本邦においても一段と広がるだろう。
- ・ また、アセット側のトークン化にかかるユースケースが広がりを見せるなか、資金側のトークン化や相互運用性の向上にニーズが存在すると認識。特に、中央銀行マネーのオンチェーン活用を効果的なものとするためには、相互運用性の向上が鍵となるだろう。

（参加者）

- ・ Project Guardian⁷では、パブリックチェーンの Polygon が利用されている。Trust Anchor⁸から検証可能な資格情報（VC）の発行を受けた保有する参加者に限り取引を実行できるようにした取り組みである。
- ・ Coinbase は、Ethereum の L2 パブリックチェーンである Base を開発した。パブリックチェーンでは、誰でもアプリケーションを作成可能であるが、Coinbase は規制のもと KYC/AML を行わなければならない、同時に、Base は誰で

⁷ Project Guardian とは、シンガポール金融管理局（MAS）が主導する、資産トークン化に関する実証プロジェクト。

⁸ Project Guardian における Trust Anchor とは、DeFi プロトコルへの参加を希望する主体に、審査・確認を行い、VC を発行する規制対象の金融機関を指す。

もアプリケーションを作成可能なオープン性を有するほか、DeFi プロトコルである Morpho⁹との連携を進めている。このように、規制に準拠した金融事業者が DeFi のようなオープンな環境へのアクセスも提供している点は、今後のブロックチェーンを考えるうえで参考となる。

- ・ Robinhood が提供する Ethereum の L2 (Robinhood Chain) は、当初、規制金融商品を取り扱っていたが、2026 年 7 月 1 日より、パブリックメインネットをローンチした。これにより、規制金融商品の世界と、誰でも DeFi を構築できるなど、オープンな世界が共通のブロックチェーン上で共存しているものと考えている。
- ・ 上述の例からも、パブリックチェーンを活用しつつ、規制要件を満たすよう KYC や商品設計、スマートコントラクト等による制御を行うことが現実的な解決策になってきている。

以 上

⁹ Morpho とは、暗号資産・ブロックチェーン領域における分散型金融プロトコルの 1 つ。ユーザー間の暗号資産の貸借を仲介するレンディングサービスを提供しており、スマートコントラクトを利用して、仲介者を介さずにデジタル資産の貸出・借入を可能にする。