

暗号資産の健全な取引を促すための法令遵守支援ソリューションの開発 「Transaction analysis solution for better compliance of cryptoassets」 －新たな経済圏に「クリーン」な暗号資産の流通を－

1 背景

暗号資産は、2017年のBitcoinの価格急騰以降、急激に社会の注目が集まることとなった。暗号資産のなかには、スマートコントラクトと呼ばれる仕組みを備えたものが存在しており、2019年後半にはこの仕組みを活用したDeFiとよばれる新たな形態の金融サービスや金融商品が登場した。DeFiにおける全世界での運用残高はすでに4兆円弱という莫大なものとなっており、新しい経済圏としての萌芽が見られる。

一方で、これだけの経済圏の急成長により、各種の規制整備や法令遵守技術の実装が追いついておらず、望ましくない経済活動が行われていることが指摘されている。具体的には、暗号資産取引所に対するサイバー攻撃によって流出した暗号資産の資金洗浄や、ダークネット等における薬物や銃器といった違法物品の売買収益の運用、テロ資金の供与などが、DeFiを介して行われているとの指摘がある。

こういった健全とは言えない経済活動を見逃す、または黙認することは、犯罪行為を助長することにほかならず、公正な投資活動への動機を奪うことに繋がりかねない。それゆえ各国における規制当局は、暗号資産を用いた経済圏において既存の金融業と同様に、流通する資産の検査体制確保や資金洗浄の防止に積極的に取り組んでいる。

2 目的

本プロジェクトは、DeFiのエコシステムが健全に発達し続けられるようにするため、資金洗浄を防止するための基礎技術を開発し、DeFiサービスの提供者が直ちに対策に取り組める環境作りを行うことを目的としている。具体的には、DeFiに投資される利用者資産の健全性を評価し、いわば「クリーン」な暗号資産だけが流通するよう、当該サービスが利用者に対するサービス提供の可否を容易に判断できるような仕組みの構築を目指した。また、本プロジェクトが提案する健全性評価手法が認知されることで、法令整備を急ぐ規制当局に対しての参考事例となることを目指した。

3 サービスの内容

プロジェクト期間においては、暗号資産の移転を準リアルタイムでデータベース化する「インポーター」、暗号資産アドレスの健全性を評価する基礎となるリスク情報を収集する「スクレイパー」、問い合わせの受付、評価と回答など、DeFiサービスとのインタフェースとなる「オラクル」と呼ばれる一連のコンポーネントを

開発した。完成したインポーターを稼働させることで、暗号資産 Ethereum の開始初期から現在に至るまでのすべての暗号資産の移転および新たに発生する移転のほぼ即時での問い合わせが可能となった。またスクレイパーによって、特定の暗号資産アドレスに関するオンラインフォーラムでの発言や Tweet、および公開された脅威情報などを半自動的に収集し、「リスク情報」として集計して検索することが可能となった。そして、テストネットと呼ばれる世界中で実稼働するテスト目的の

ブロックチェーン上にオラクルを配置し、当該オラクルがテスト用暗号資産によって手数料の支払いを受け付けて、また特定のアドレスに関する健全性を数値評価した「リスクスコア」の問い合わせに対し回答できることを確認した。

これらのシステムは DeFi サービスがプログラマ的にオラクル コントラクトのメソッドを呼び出して利用することを想定しているが、一般ユーザーからも本サービスを利用できるよう、ユーザー インタフェースとなるデモ目的の Web アプリケーションを作成した。ユーザー インタフェース上で、ユーザーがリスクスコア取得対象のアドレスを入力し、問い合わせボタンを押すと、ユーザーのウォレットからオラクル コントラクトに手数料を移転し、オラクル コントラクトに問い合わせを行うトランザクションを発行する。そして、一定時間後にユーザーが結果取得ボタンを押すと、リスナーが発行したトランザクションによってオラクル コントラクトに格納された回答が読み込まれ、画面上に表示される（図 1）。

4 新規性・優位性

本プロジェクトが提唱するリスクスコアの手法は、国外のいくつかの分析企業等も提供を行っており、暗号資産を扱う一部の取引所や決済事業者では導入されてきた実績がある。しかしながら、既存サービスを DeFi がそのまま利用するには複数の課題があった。一つは技術的課題であり、もう一つはビジネスモデル上の課題である。本プロジェクトではこれらの解決に取り組んだ。

技術的課題としては、既存サービスによるリスクスコアの提供は REST API を通じて行われていたことに起因しており、DeFi はブロックチェーン上で動作する分散アプリケーションであることから、これを直接利用することができないという点

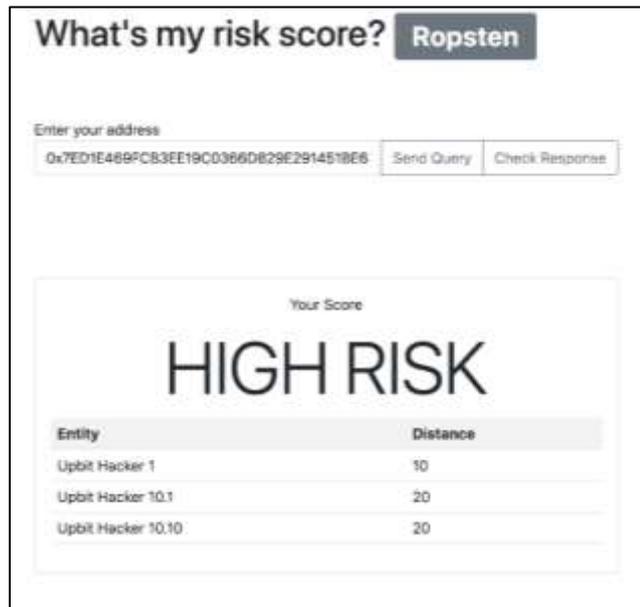


図 1 リスクスコアが高い場合の表示

であった。そこで本プロジェクトでは、オラクル コントラクトを作成することでブロックチェーン上に問い合わせ用のエンドポイントを作成し、DeFi が容易にリスク スコアの問い合わせを行えるようにして、この課題を解決した。

ビジネス モデル上の課題としては、既存サービスは企業等の組織を対象ユーザーとして、年間契約のもとで銀行振込による毎月精算、というような形態を採っていることが一般的だったところ、ブロックチェーン上で自律的に実行される DeFi は、利用者による民主的なガバナンスで共同管理されていることが多く、運営組織の存在を前提とした従来の課金方法は必ずしも適さないという点であった。また既存サービスの固定金額制によるしばしば高額な利用料設定は、利用者が頻繁に増減する DeFi において馴染まないという課題があった。そこで本プロジェクトでは、サービス利用のたびに暗号資産によってオラクル コントラクトに利用料を支払える仕組みを導入して DeFi から利用しやすい課金制度とすることで、この課題を解決した。

このように DeFi へリスク スコアを提供する際に発生する課題を解決したことは、既存サービスと比較した際の本プロジェクトの重要な優位性である。またさらに DeFi からリスク スコアを利用できるようにした試みは本プロジェクトが初であり、新規性を有する。

5 事業普及（または活用）の見通し

本プロジェクトでは、提携する DeFi サービス事業者の選定を試みたが、限られた期間においては達成に至らなかった。代わりにマーケティングの一貫として、本プロジェクトのコンセプトを実証する 2 つのコンセプト DeFi サービスを自ら構築した。これらのサービスはリスク スコアをサービス運用に活用しており、オラクル コントラクトがどのように機能するか、組み込みがどれだけ単純か、手数料をどのように支払うか、DeFi サービスと利用者にとってどのような便益をもたらすのか、などを示すことを目的とした。ただし、資金決済に関する法律で定められた暗号資産交換業に関する規定等に抵触することを避けるため、暗号資産としての価値がないテストネット上でのサービス リリースにとどめた。

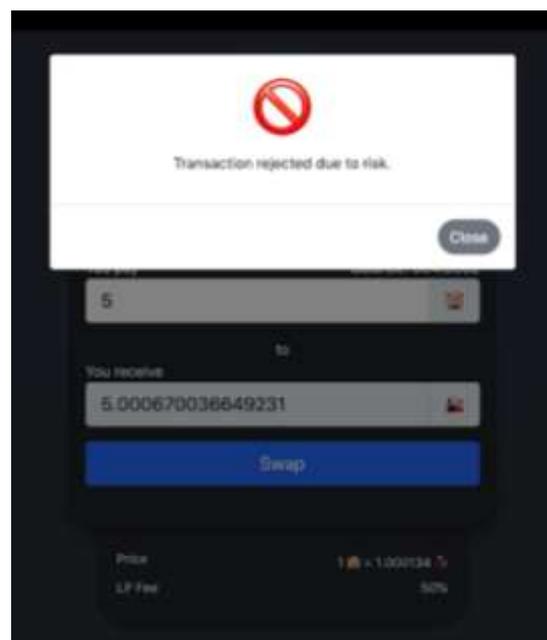


図 2 リスク スコアを活用したトークン スワップ サービス例

1つ目は、ある暗号資産を別の暗号資産に交換するトークン スワップ サービスである。このサービスは、過去の犯罪に関与したことが判明しているアドレスからの交換要求である場合、処理中にユーザーの要求が却下されるよう（図 2）、オラクル コントラクトと対話する。これにより、不正な収益として得られた暗号資産が別の暗号資産に変換される資金洗浄が行われることを防止できることを示した。

2つ目は、ある暗号資産を担保にして、別の暗号資産を借り入れる融資サービスである。このサービスは、融資実行の時点でユーザーのリスク スコアを判定し、リスク スコアの低いユーザーには優遇された金利が適用されるよう、オラクル コントラクトと対話する。これにより、ユーザーのリスク スコアが低いことが、ユーザーの直接的な利益に繋がり、健全な取引を行うことに対するインセンティブとなりうることを示した。

これらのコンセプト DeFi サービスは、本プロジェクトの開発手法を利用することの利点を示すショーケースになったと考えている。今後 DeFi コミュニティに対する普及活動や継続的なロビー活動のために、ユーザー・サービス事業者・規制当局のそれぞれに付加価値を創出するサービス例として、保守および運用を続けていく。

6 期待される波及効果

前述したとおり、本プロジェクトが開発したサービスは、DeFi サービスに容易に組み込むことができ、また DeFi のユーザーに直接のおよび間接的に利益をもたらす。これらのことから、今後誕生する DeFi サービスによって積極的に採用されることを期待しており、また本サービスを利用する DeFi サービスをユーザーが優先して選択するようになることを期待している。実現すれば本サービスがより広く普及する好循環が生まれる。

さらに、本サービスが目指す資金洗浄への対策という目的は、少数国だけの導入ではなく世界的に導入されることで効果が最大化される。よって、DeFi を対象とした資金洗浄への対策手法が規制当局によって広く認識され、本サービスの開発手法の導入が、国際的に標準的な規制として普及することを期待している。

7 イノベータ名（所属）

竹井 悠人（株式会社 Basset）、WALRAVEN AYA ASHLEY（株式会社 Basset）、KARAMATOV NAVRUZBEK（株式会社 Basset）、平元 尚貴（東京理科大学）

8 （参考）関連 URL

<https://safedefi.work/>