分散型金融（DeFi）におけるリスクとトラスト構造に関する考察

分散型金融（DeFi）の市場が急速に発展するに連れ、各国規制当局による規制の議論が加速している。様々なステークホルダーやシステムが互いに連携しシステム全体で機能する分散型金融においては、各要素のリスクとトラスト構造を踏まえたうえでシステム全体としてのガバナンスが問われる。

加速する分散型金融市場と各国規制の議論

ブロックチェーン（以下、BC）技術等を用いて中央機関による管理を廃してP2Pで金融取引を実現する分散型金融（Decentralized Finance：以下、DeFi）の市場が急速に発展しており、既に1,000億ドル前後の暗号資産がBC上のコントラクトにロックされている[1)]。

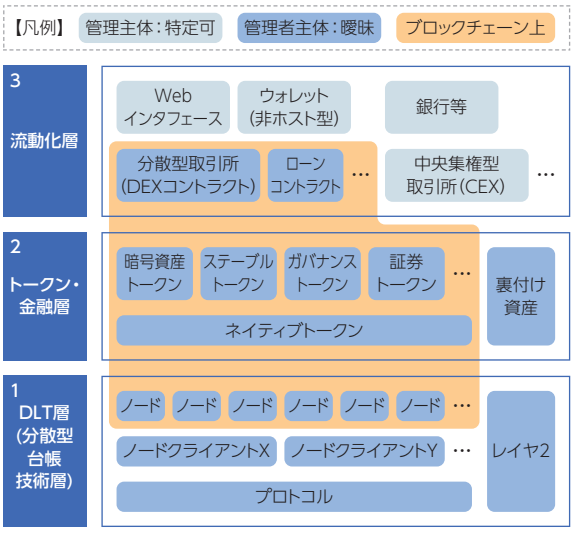
また市場拡大に連れた規制の議論も活発化しており、金融活動作業部会（FATF）は2021年10月に暗号資産に関するガイダンス[2)]の改訂版を公表し、DeFiのソフトウェアや技術自体は規制対象にならないとしつつも、DeFiに対する支配力や影響力を有する場合は、その取り決めが分散化しているように見えたとしても規制される可能性があるとの見解を示した。また、日本においては金融庁が「デジタル・分散型金融への対応のあり方等に関する研究会」において「複数レイヤー全体を管理する主体が存在しない場合であっても、サービスが幅広く利用されるためには、システム全体が技術・契約・制度・インセンティブ・信頼等によって規律付けられる必要があり、規制の名宛人として管理責任を果たせる立場にある者がこうした状態を実現する必要がある[3)]」と中間整理している。本稿ではシステム全体で規制をかける主体がいないDeFiの構成要素を分解し、各要素におけるリスク分析からDeFiのトラスト[4)]構造を整理したい。

分散型金融の各構成要素のリスクとトラスト構造

本稿では、DeFiにおける構成要素を①DLT（分散型台帳技術）層、②トークン・金融層、③流動化層に分類した上で、それぞれの構成要素のリスクを整理した。

まず、①DLT層ではブロック生成やコンセンサス等のルールをプロトコルとして規定したうえで、OSSコミュニティや開発企業がプロトコルをノードクライアントとして実装し、各参加者は各自のサーバーでノードクライアントを稼働してBCネットワークが構成される。ここで、プロトコルについては単一の主体ではなく、コミュニティで議論がなされるため**様々なステークホルダーの思惑により仕様が決まり、時に意見の不一致からプロジェクトが分離することもあるし、ノードクライアント実装においてはバグの混在が問題になり得る。**また、**ノードが互いにデータ通信をする必要性等から処理性能に限界がある。**このため、BCの外（レイヤー2）でデータを処理し性能向上する手法が次々に提案[5)]されているが、**それぞれ制約や課題が存在する。**またBCネットワークの参加者を増やすために、プロトコルで定

図表　DeFi構成要素の簡略図



(出所) 野村総合研究所

NOTE

1) 出典：DeFi Plus（2021年11月30日時点）。
なお、2020年9月号の「分散型金融（Decentralized Finance）がもたらす新金融の可能性」の調査時点では40億ドルだった。
2) 出典：2021年10月28日FATF「暗号資産及び暗号資産交換業者に対するリスクベース・アプローチに関するガイダンス」。
3) 出典：2021年11月17日金融庁「デジタル・分散型金融への対応のあり方等に関する研究会」中間論点整理。
4) 先の金融庁の中間論点整理においては、システム全体の規律付けがなされている状態の例として「システムへの参加者等における「トラスト」が存在している状態が確保されていること」を挙げている。
5) State Channel、Plasma、Rollup等。
6) 例えば、マイニングが特定の国に偏っている場合に、その国の政府がマイニング業者の差し押さえをすることでブロックチェーン全体が支配される等。
7) 例えばapp.uniswap.orgではUniswapコントラクトにアクセスするためのWebが運営されている。規制等への対応としてWebで扱うトークンを制限する動きも見られる。
8) 分散化の度合いを定量化する手法として、Coinbase元CTOのBalaji Srinivasanが提唱したNakamoto Coefficientが使われることがある。
9) ここでは各中央管理者が担っていた機能がDeFi機能として分離する。

めたルールに従いインセンティブとしてネイティブトークン等をマイニング報酬として配布することが一般的だが、**マイニングする主体が過度に偏るとプロトコルが恣意的に操作されたり、BCが分岐（フォーク）したり、場合によっては特定の国の政府にマイニングがコントロールされるリスク[6]も発生するかもしれない。**

次に、②トークン・金融層では前述のネイティブトークンに加えて、様々な仕様の商品コントラクトのコードを“誰か”がBCに配置することで、トークンや金融機能が利用可能になるが、スキームによってはトークンの裏付け資産が銀行等で管理されたり、トークンが議決権を有してガバナンスの役割を果たしたりすることもある。**ここでもコントラクトコードにはバグ混入のリスクがあるし、また、コントラクトを生成した主体が特権的に資産を管理したり、裏付け資産が適切に管理されない等の問題も発生している。**

最後に、③流動化層では、秘密鍵を用いてトークン等の移転を提供することで市場に流動性を付与している。ここでは特定の事業者が運営する暗号資産交換業者に加えて、分散型取引所コントラクト（DEX）、投資家が秘密鍵を管理する非ホスト型ウォレットや、Webやアプリ等のインタフェース[7]が連携することでDeFiへのアクセスが実現される。ここでは**秘密鍵の漏洩や搾取が度々問題になるし、また特定の管理主体がいない分散型取引所でのP2P取引によるマネー・ロンダリング/テロ資金供与対策（AML/CFT）上のリスクも存在している。**

このようにDeFiでは各レイヤーの各要素で、異なる主体が異なるリスクを内在しながらシステム全体が機能している。これらのリスクに対して、コードの監査やバグバウンティの実施、各種分散化[8]（マイナー、ノードクライアント種類、開発者、取引所、トークン保有者、ノード設置国等）、不正を抑止するためのインセンティブ設計、投資家を保護するための現実世界の法規制や契約等が、各要素で対策されることが期待される。つまり、各要素での“トラスト”が積み重なることでDeFi全体のトラストが成り立っているとも言える。しかし、従来の金融にある責任分解などの取り決めも曖昧だし、特定の運営主体が存在しない以上、従来の金融における単一主体に対する規制も難しいという点で、規制の議論が難航する原因にもなっていると想定される。

このように現状のDeFiは様々なリスクを抱えてはいるものの、プラットフォーム全盛時代であるWeb2.0から自己主権型のWeb3.0へのパラダイムシフトの1つとしてDeFiが拡大してきた側面もあり、過度な集中による金融リスクの高まりの可能性も踏まえるとDeFiのアーキテクチャから学べることは少なくないのではないだろうか。

日本では複数の金融機関がコンソーシアム型のBCを活用しDeFiへの一歩を踏み出しているが、コンソーシアム型では中央集権要素を残すことで規制対象や責任主体の明確化が可能な反面、BCの価値であるオープン性が限定されてしまう面もあり、今後、金融機関においてもオープン化やプロトコル化[9]の議論が進む可能性はあり得る。今後、市場の発展に連れ、規制とイノベーションのバランスがますます問われていくだろう。

Writer's Profile

周藤 一浩 Kazuhiro Sudo
金融デジタルビジネスデザイン部
上級コンサルタント
専門はブロックチェーン、証券トークン/暗号資産/ペイメント
focus@nri.co.jp