

暗号資産における分散型金融

— 自律的な金融サービスの登場とガバナンスの模索 —

決済機構局 北條真史、鳩貝淳一郎

Bank of Japan Review

2021年4月

分散型金融は、パブリック型ブロックチェーン上に構築された暗号資産の金融サービスであり、特定の仲介者や管理主体を必要とせず自律的に運営され、サービスの利用や提供を容易に行えるという特徴を持つ。近年、利用が急増しているが、利用者のニーズに応える新たな金融サービスを生み出す可能性などとともに、課題やリスクも指摘されている。分散型金融は責任主体が曖昧であり従来の規制アプローチのみでは政策目的が十分に達成できない可能性も指摘されており、各国の規制当局は、遵守すべきルールの策定とともに、幅広いステークホルダーとの対話を通じた実効性のあるガバナンスを模索している。将来的に暗号資産市場と既存の金融市場の結びつきが強まり、金融・決済システムや金融市場の安定の観点から暗号資産市場の重要性が高まる可能性も踏まえると、イノベーションとリスクの両面を意識しつつ、暗号資産市場や分散型金融の動向を注視していくことが重要である。

はじめに

分散型金融 (Decentralized Finance, DeFi) は、暗号資産市場において、様々な金融サービスをプログラムにより自律的に提供する仕組みである。確立した定義は存在しないが、特定の管理主体を必要としないパブリック型ブロックチェーン上で¹、スマートコントラクトを活用して構築・運用される暗号資産の金融サービスを指す (以下、本稿では、ブロックチェーンはパブリック型を指す)。

スマートコントラクトとは、ある条件で作動するプログラムをブロックチェーンに登録し、条件が満たされた際に自動的に作動させ、その結果をブロックチェーンに自動的に記録する仕組みである²。この技術により、特定の仲介者や管理主体を必要としない形で、金融サービスが自律的に提供される。

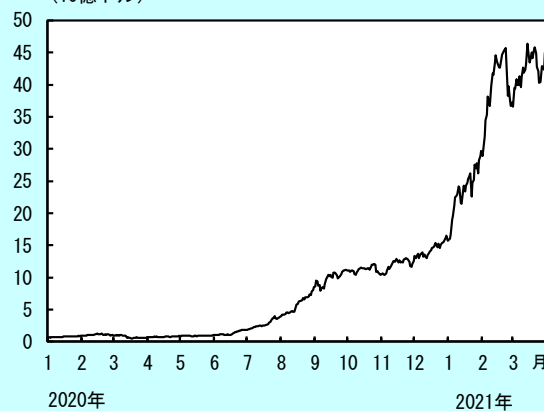
分散型金融はその利用が広く開放されており、また、プログラムを開発しスマートコントラクトとしてブロックチェーンに登録・公開することで、自由に新たなサービスを提供できる。プログラムの作動状況やプログラムによって実行された取引結果などもブロックチェーン上で公開され、誰でも参照できる。

現在、分散型金融による金融サービスが数多く提供されており、暗号資産の交換、暗号資産の貸

出から、カストディ、保険、デリバティブ、予測市場まで、200以上が存在する。ビットコインをはじめとする暗号資産の価格が上昇し需要が高まるなか、暗号資産の貸借を容易にしたり、買い持ち以外の多様な運用手段を提供したりすることで投資家を引き付けている。実際、分散型金融サービスの利用 (暗号資産の運用残高) は昨年央以降に急増し³、本年3月時点で400億ドル (約4兆円) に達している⁴ (図表1)。

【図表1】分散型金融サービスのTVL

(10億ドル)



(注) TVL (Total Value Locked) は、代表的な分散型金融サービスに預けられている (ロックされている) 暗号資産の総額。

(出所) DeFi Pulse

本稿では、代表的な分散型金融サービスを挙げ、潜在的なメリットと課題の両面を説明する。続いて、分散型金融の持つ特質のために、従来のアプローチでは実効的な規制を行うことが困難との指摘を紹介した上で、分散型金融のガバナンスに関する規制当局の国際的な取組みを概観する。

代表的な分散型金融サービス

近年多くの利用者を集めている代表的なサービスとして、DEX とレンディングがある⁵。

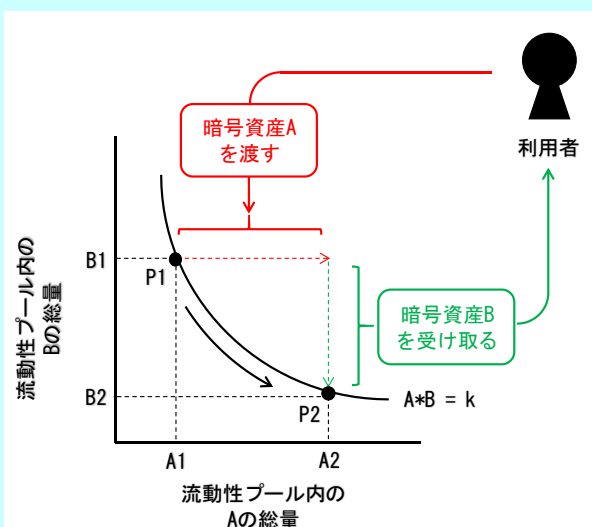
(DEX : Uniswap の例)

DEX (Decentralized Exchange、分散型取引所) は、暗号資産同士を交換する取引所の機能を、スマートコントラクトにより自律的に提供するサービスである。DEX は現在多くのサービスが存在しており⁶、なかでも比較的后発の Uniswap と呼ばれるサービスがシェアを伸ばしている。Uniswap では、取引価格の決定や市場流動性の管理などの機能がスマートコントラクトにより実装され、マーケットメイクも自律的に行われる⁷。

Uniswap の機能を、「暗号資産の交換」と「流動性の供給」の2つに分けて説明する。暗号資産の交換においては、利用者は、暗号資産のペアごとに存在する「流動性プール」の中から交換したい暗号資産ペアのプールを選び、自身の暗号資産を差し出して、目的の暗号資産を得る(たとえば「暗号資産 A と B」の流動性プールに対し、A を送り目的の B を得る)。交換レートは、プール内の当該暗号資産ペアの残高の積が、取引の前後で一定になるように自動計算される(図表 2)。

このような交換は、流動性プールに暗号資産のペアが十分に準備されていることを前提としている。利用者は流動性プールに対して暗号資産ペアを預け入れることで流動性を供給することができ、その際、報酬として Uniswap より「流動性トークン」を受領する(図表 3)。利用者は流動性トークンと引き換えに暗号資産ペアの返還をいつでも受けることができ⁸、その際 Uniswap より報酬(暗号資産の交換において利用者が支払った手数料が原資)を受け取る。利用者は、任意の暗号資産ペアについて、新たな流動性プールを作ることができる⁹。

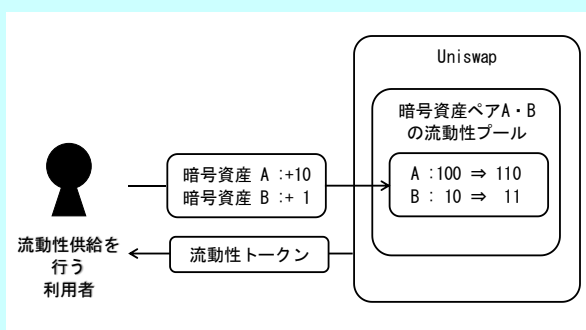
【図表 2】 Uniswap における暗号資産の交換



- ・流動性プール内の A と B の残高の組合せを、点 P1 とする。
- ・流動性プールに対し暗号資産 A を渡すと(上図中の赤字)、暗号資産 B を受け取る(上図中の緑字)。ここで得る B の量は、「流動性プール内の暗号資産の A と B の残高の積」が取引の前後で一定になるよう自動計算される。
- ・この取引後、流動性プール内の A と B の残高の組合せは点 P2 となり、同量の A を渡して交換できる B の量は減少する。これは Uniswap において「A 安 B 高」が進んだことを意味し、他市場の交換レートとの乖離が生じる。
- ・その結果、Uniswap において「B を渡し A を受け取る」取引の魅力が他市場より増す。裁定取引が行われ、Uniswap の交換レートは「A 高 B 安」の方向に進む(残高の組合せは点 P2 から左上方向に進む)。

(出所) Uniswap ウェブサイトをもとに作成

【図表 3】 Uniswap における流動性供給



- ・利用者は、流動性プールに対し暗号資産ペアを預け入れ、その額に応じて Uniswap から流動性トークンを受領する。
- ・流動性供給を行った利用者は、流動性トークンと引き換えに、預け入れ相当額の暗号資産の返還を受け報酬を得る。

(出所) Uniswap ウェブサイトをもとに作成

(レンディング：Compound の例)

レンディングは、利用者から暗号資産を預かりこれを貸し出す機能を、スマートコントラクトにより自律的に提供するサービスである。

代表的サービスである Compound では、貸し手は暗号資産を流動性プールに担保として差し入れ（ロックし）、これと引き換えに預かり証の役割を果たす「cToken」を受領する。貸し手はいつでも cToken を戻して、預け入れた暗号資産に利息を加えた額を回収できる（図表 4）。cToken の保有者は借り手になることができ¹⁰、この場合 cToken を担保として預け入れ、暗号資産を流動性プールから借り入れる（図表 5）。借り手は、いつでも借入額に利息を加えた金額を流動性プールに対して返済できる。

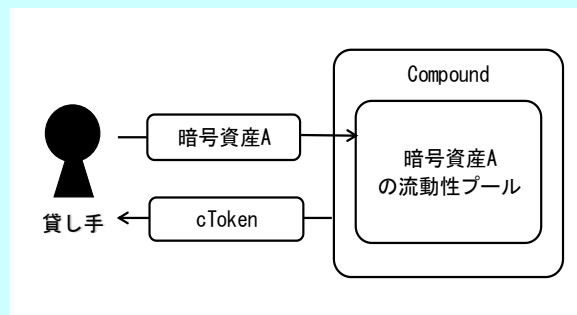
利息や手数料は、流動性プールでの暗号資産の需給をもとにリアルタイムで自動計算される。未収利息の増加や流動性プールに差し入れた担保の価格下落などにより、利用者の借入額が借入限度額を超過した場合、追加的な担保差し入れがないと、差し入れ済みの担保は市場価格から一定割合を割り引いた価格で清算されることになる。

分散型金融サービスを用いた運用の実態

(イーロドファーミング)

最近では、数多くの分散型金融サービスの手数料・利率・交換レートなどのモニタリングを行い、サービス間の裁定機会を捉え取引を行う利用者が増えている。たとえば、暗号資産 A を Uniswap で B に交換し、B を他の DEX で C に連鎖的に交換することに裁定機会があると認識したものの A を保有していない利用者が、即座にレンディングサービスで A を借り入れて一連の取引を行うといった例が挙げられる。また、レンディングサービスに担保を差し入れて借り入れた暗号資産を、再度担保として暗号資産を借り入れることを繰り返し、レバレッジを利かせて大きなポジションを造成することもある。なお、これらを通じて得られる流動性トークンや cToken は、暗号資産として分散型金融サービスで運用することができる。このように分散型金融サービスを組み合わせ、高い利回りを求めて暗号資産を運用する行為は、イーロドファーミング（利回り農業）と呼ばれる。

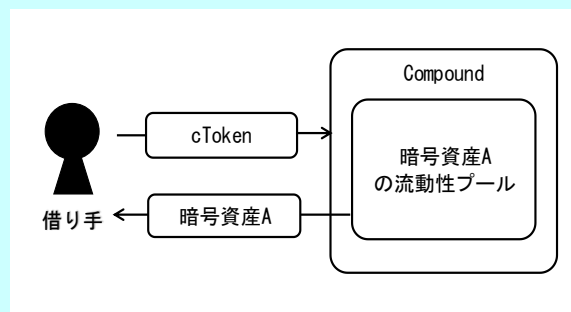
【図表 4】 Compound への暗号資産の貸出し



- ①貸し手は、保有する暗号資産 A を Compound の流動性プールに預け入れる。
- ②設定された交換レートに基づき、暗号資産 A に紐づいた cToken が貸し手に交付される（たとえば、暗号資産 Ether がロックされた場合、cEther という cToken が交付される）。
- ③貸し手は、任意のタイミングで、cToken を Compound に戻し、暗号資産を回収する。
- ④その際、預け入れ額より利息分だけ多く回収できる。

(出所) Compound ウェブサイトをもとに作成

【図表 5】 Compound からの暗号資産の借入れ



- ①借り手は、保有する cToken を担保として Compound に預け入れる。
- ②担保額に担保掛け目を乗じた借入可能額を上限に、Compound の流動性プールから暗号資産が貸し出される。
- ③借り手は、任意のタイミングで、借り入れた暗号資産を流動性プールに返済し、cToken を回収する。
- ④その際、借入額より利息分だけ多く返済する。

(出所) Compound ウェブサイトをもとに作成

最近では、分散型金融サービスの価格や手数料などの相場情報を幅広く集約し、多くのサービスを組み合わせ最良のリターンを得られるよう暗号資産運用を代行する「アグリゲーター」と呼ばれるサービスも登場している。この中には、スマートコントラクトによって動作し、これ自体が分散型金融サービスとなっているものもある。

（ガバナンストークンと流動性マイニング）

一般に、分散型金融サービスの立ち上げ時には、開発・運営者が担保掛け目や手数料の算出方法などの重要事項を決定する。しかし、これらの重要事項の決定を、利用者・開発者のコミュニティに委ねていく方針を打ち出しているものもある。

その具体的な方法として、ガバナンストークン（DeFi トークン）と呼ばれる投票権を表象するトークンが、利用者に対して付与される。ガバナンストークンの持ち主はその持ち分に応じて、投票権や案件の提案権を得る。前述の Compound では COMP トークンが、Uniswap では UNI トークンが、利用者（流動性供給を行う者を含む）に対し発行されている。

ガバナンストークンは、本来、重要事項に関する投票権を表象するものであるが、最近では、その値上がり期待から投機的需要を引き付け、中央集権型取引所や分散型金融サービス上で盛んに取引される事例がみられる。ガバナンストークンを入手するために流動性供給が盛んに行われており、その行為は流動性マイニングと呼ばれている¹¹。

このようなイールドファーミングや流動性マイニングの動きが、最近の分散型金融サービスにおける取扱高や運用残高の増加の一因になっているとの指摘がある。

（投機的需要に乗じた利益確保）

分散型金融のプロジェクトの中には、短期的な利益の獲得を目的にサービスを設立する事例も見られる。たとえば、分散型金融サービスではプログラムの内容が公開されているため、これを参照して類似サービスを容易に立ち上げ、そのガバナンストークンを DEX に上場し、投機的需要が生じて価格が上がったところで早々に売り抜けて収益を確定するというケースがある。ガバナンストークンは分散型金融サービス設立者などが

予め一定割合を保持していることが多い。サービス設立者が立ち上げ早々にトークンを大量に売却したという事実が判明し、ガバナンストークンの価格が急落した事例もある。

分散型金融の潜在的なメリットと課題

分散型金融については、金融システムに競争をもたらす可能性や潜在的なニーズを捉えた新規サービスの創造の可能性などのメリットが指摘される一方、利用者保護の問題やスマートコントラクトが不具合を内包する可能性といった課題やリスクも指摘されている。

（分散型金融の潜在的なメリット）

① 競争をもたらす可能性

金融安定理事会（Financial Stability Board, 以下FSB）による報告書¹²、分散型金融技術¹³には「金融システムに競争の拡大と多様性をもたらす可能性がある」としている。別の論考では¹⁴、分散型金融では金融インフラ（カストディアン、エスクローエージェント、中央清算機関）の役割が自律的なプログラムによって担われることから、第三者による監査の必要性が低減される可能性や、こうしたこともあって分散型金融の運営が既存の金融インフラに比べて効率的となる可能性が指摘されている。

② 新たなサービス創造の可能性

前述のとおり、分散型金融では容易に新規サービスの立ち上げができるため、実験的な試みを繰り返し行うことができる。単一のプラットフォーム（イーサリアム）の上に構築されているため、複数のサービスを組み合わせ新規サービスを立ち上げることもしやすい。こうした特性から、潜在的なニーズを捉えた新規サービスを生み出しやすい可能性を有していることが指摘されている。

③ アクセシビリティが向上する可能性

分散型金融サービスは、誰でもどこからでもインターネットを通じて利用でき、金融サービスへのアクセシビリティが向上する可能性が指摘されている¹⁵。

① 利用者保護

分散型金融においては、中央集権型取引所のような上場審査がなく、流動性が低いものも含め様々なトークンが取引され、値動きについても既存の金融商品とは異なっている。また、レバレッジに関する規制もない。前述の FSB の報告書も、分散型金融における利用者の保護に関する不確実性を指摘している。

現在、分散型金融で積極的に運用を行っている利用者は、暗号資産の技術や運用方法に精通した層にとどまっている。もっとも、ユーザーインターフェースの改善が進んでおり、必ずしもリテラシーが高くない利用者が増えていく可能性がある。また、投機熱が高まると、そうした利用者が集まりやすくなる。

② スマートコントラクトの不具合と影響拡大

既存の金融サービスでは、システムに不具合が見つければ、運営者が一時的にサービスを停止して被害の拡大を抑えつつ不具合を修正することができる。しかし、スマートコントラクトに内包された不具合や脆弱性が顕現化して損失が生じた場合でも、自動的に動作し続けるため、外部からサービス停止や取引の巻き戻しなどの対応を行うことは難しい。スマートコントラクトの検証が必ずしも十分でないまま、サービスの提供を急ぐ事例も散見され、懸念が示されている。

こうした不具合が顕現化した場合、その悪影響は分散型金融サービス間の依存関係によって、他サービスにも拡大する可能性がある。イーロードファーマーミングの項で説明したとおり、分散型金融では、暗号資産をあるサービスに預け入れてトークン A を得て、これを別のサービスに預け入れてトークン B を得て、さらに別のサービスに預ける、といった行動が複数のサービスにまたがって行われている。結果、1 つのサービスで不具合が顕現化して、あるトークンの価格が急落した場合、その影響が多くのサービスや投資家に波及する可能性がある。その影響の度合いは、高レバレッジで取引している利用者が多いほど大きなものとなる。

(実効的な規制の難しさ)

前述のとおり、分散型金融はメリットとともに様々な課題やリスクを内包している。一方で、規制対応を取ろうとしても、分散型金融が持つ特徴により実効性の確保が難しいとの指摘がある(図表 6)。

まず、分散型金融は、特定の運営者・仲介者が不在で、サービスが分散化された主体に担われており、容易にサービスを開始・利用でき、匿名性も高いことから、規制の対象や責任主体の特定が困難となっている。また、インターネット上で運用されグローバルな性質を持つため、規制が不十分な法域があればそこが抜け穴となる。加えて、規制で禁止しようとしても自律的に稼働し停止不能であるうえ、改竄耐性が高く不正があっても後から修正するという方法を取ることが難しい。こうした性質から、既存の規制手法では十分な実効性が発揮されにくいと指摘されている。

【図表 6】分散型金融の特徴と規制上の含意

特徴	規制上の含意
分散化が進んでいる	・特定の仲介者や管理者が不在で、サービスは分散化された不特定の主体に担われている。
オープンである	・誰もがサービスを利用でき、また開始できる。
匿名性が高い	・取引に用いられるアドレスと利用者情報は直接に紐付けられていない。 ・匿名性を高める技術の開発も進展。
グローバルである	・サービスに問題があっても、規制が不十分な法域を抜け穴として世界中にサービスが提供されうる。
自律性が高い	・規制で禁止しても、自律的に稼働する。
改竄耐性が高い	・不正があっても事後的に修正することが困難。

(出所) 日経フィナンシャル「『分散型台帳』が創る金融新秩序 規制も共創時代」(2020年10月10日)、牛田遼介「分散型金融におけるガバナンス」(2020年10月)などをもとに作成

（規制に関する国際的な議論）

こうした分散型金融の特徴を踏まえ、各国の規制当局は、様々な取り組みを行っている。

マネーロンダリング・テロ資金対策などにおける国際協調のための政府間会合である金融活動作業部会（Financial Action Task Force on Money Laundering, FATF）は、本年、暗号資産および暗号資産交換業者の規制ガイダンスの改訂案を公表し市中協議を開始した¹⁶。同改訂案では、法人・個人が DEX などのブロックチェーン上のプログラムに関与し、顧客に代わって取引を執行するなどの機能をビジネスとして提供しているとみなされる場合、「暗号資産サービス提供者」（virtual asset service provider, VASP）としていわゆる「トラベルルール」などの遵守を求められる可能性があるとしている（トラベルルールは、業者に対し「顧客の暗号資産の移転に際し、移転元・移転先に関する情報を取得し、移転先が利用する業者に通知すること」を求める規制）。

加えて規制当局は、従来と異なる規制のアプローチも模索している。この過程では、分散型ネットワークであるインターネットのガバナンスが、多様なステークホルダーの協調により担われてきた経験が参照されている（BOX 参照）。

前述の FSB の報告書は、金融規制当局と幅広いステークホルダー（エンジニア、企業、アカデミア、投資家、サービス利用者など）との対話が早い段階から行われると、分散型金融技術の初期デザインにおいて、金融規制など公共政策上の目的が考慮されやすくなるとしている。また、インターネットのガバナンスに関する国際機関が、広範なステークホルダー間でのアーキテクチャにかかる合意形成を促した例として IETF、ICANN、W3C などを挙げ、分散型金融技術がもたらしうる新たな金融システムのガバナンス検討には、こうした先例に学ぶことが重要としている（図表 7）。

2019 年に福岡で開催された G20 財務大臣・中央銀行総裁会議の声明には、同報告書を受け、「分散型金融技術、それが金融安定性や規制、ガバナンスにもたらす潜在的な影響、及び当局が広範なステークホルダーとの対話をどのように強化できるかについての FSB の報告書を歓迎する」との記述が盛り込まれた。また、その後の G20 大阪首脳宣言にも、同趣旨の文言が記載された。

【図表 7】 インターネットのガバナンスに関連した国際機関の例

IETF (Internet Engineering Task Force)	<ul style="list-style-type: none">・インターネットのプロトコル（TCP/IP、HTTP）など、アーキテクチャや運用に関する技術の標準化を行うコミュニティ。・コンピューターサイエンスの技術者の少人数の会議体から発展。個人の資格で参加。
ICANN (Internet Corporation for Assigned Names and Numbers)	<ul style="list-style-type: none">・インターネットのドメイン名、IP アドレスなどの資源を、グローバルに管理・調整する民間の非営利法人。・上記の資源管理に関する監督権限は、米国政府商務省から委譲された。
W3C (World Wide Web Consortium)	<ul style="list-style-type: none">・Web 技術の標準化を行う産学官コンソーシアム。HTML や XML などの仕様を策定。

（出所）Financial Stability Board 報告書、各機関のウェブサイトなどをもとに作成

本邦金融庁は、これらの国際的な議論に積極的に参画している。加えて、分散型金融技術がもたらしうる新たな金融システムについて、イノベーション実現と規制目的の両立に向けたオープンな議論を、幅広いステークホルダーの間で進めるべく活動している。一例として、2020 年 3 月に発足したブロックチェーンに関するグローバルなネットワーク BGIN（Blockchain Governance Initiative Network）に、多様なステークホルダーとともに参加していることが挙げられる。BGIN では、イノベーションと規制（前述の FATF トラベルルール対応など）の両立に向けた文書の作成を目指すワークストリームが立ち上がっている。

おわりに

分散型金融は、近年幅広いサービスが提供され利用の裾野が広がっている。これらはブロックチェーン上のスマートコントラクトにより自律的に動作しており、たとえば DEX やレンディングでは、利率や手数料の算出から担保の清算に至るまで、様々な機能が自動化されている。

分散型金融の潜在的なメリットとして、金融システムに競争をもたらす可能性、新たなサービスの創造の可能性、アクセシビリティの向上などが指摘されている。利用者保護に関する不確実性や、

様々な脆弱性が顕現化した際の影響が拡大しやすいなど、リスクや課題も存在する。

こうしたリスクや課題を内包する一方で、サービス開始や利用が容易で、匿名性も高く、責任主体が曖昧となっていることなどから、規制の執行が困難である点が指摘されている。規制当局は、暗号資産に関わるビジネスが遵守すべきルール
の策定とともに、分散型金融の特質も踏まえた新たな規制アプローチを模索している。サイバー空間のガバナンスの議論を下敷きに、実効性のあるガバナンスを幅広いステークホルダーと共に目指す動きがグローバルに進展しつつある。

現在、ビットコインほか暗号資産の価格が高水準となり市場規模も拡大するなか、機関投資家が暗号資産市場に参入しているとの指摘がある。海外では暗号資産ETFが上場されるなど、投資が以

前より容易に行える環境になりつつある。ブロックチェーンを活用して、伝統的な金融商品を含む様々な資産の市場を創設する試みも進展している¹⁷。仮に将来的に、既存の金融市場の参加者による暗号資産の投資が大きく増加した場合や、伝統的な金融商品と暗号資産の交換が技術的に容易になった場合には、暗号資産市場と既存の金融市場の結びつきが強まり、金融・決済システムや金融市場の安定の観点から暗号資産市場の重要性が高まる可能性がある。

暗号資産市場や分散型金融については、イノベーションなどの可能性とリスクの両面を踏まえつつ、市場動向、技術の進展、ガバナンス改善に向けた取組みなどを、今後も注視していくことが重要である。

BOX サイバー空間のガバナンスの議論とブロックチェーンへの応用

インターネットにより成立したサイバー空間は、単一の管理者がおらず、様々なガバナンス上の問題に直面してきた。この問題解決のために展開された議論や経験は、分散型金融の健全な発展にも示唆を与えるとの指摘がある¹⁸。サイバー空間における規制については、米国の法学者レッシグ (Lawrence Lessig) の議論が参照されることが多い。レッシグは、個人の行動を規制するメカニズムを、①国家によって制定される「法」、②経済的動機に裏付けられた「市場」、③社会によって規定される「規範」、および④「アーキテクチャ」(後述)の4つに整理した¹⁹。

たとえば、ある場所への立ち入りを規制したい場合、政府は、立法により立ち入りを禁じる(法)、立ち入らない場合に報酬を与える(市場)、「この場所に立ち入ることは悪いことだ」という規範を作る(規範)、といったことができる。加えて、その場所を壁で囲んで立ち入れなくすることもできる(アーキテクチャ)。政府は、最も効果的に目的を達成できるよう、有限な資源を4つの規制メカニズムに配分する。規制メカニズムのうちアーキテクチャの概念がやや難しいが、行為者の遵法意識、経済合理性、倫理観などの有無によらず「そもそもある行為ができない」(または自然に回避される)ような仕組みを組み込むことと解釈される。レッシグは、例として、政府が国民にシートベルトをより着用させたい場合に、シートベルトを着用しないと発進できない仕組みを乗用車に組み込むことを挙げている。

レッシグは、前述の4つの規制メカニズムは、物理空間のみならずサイバー空間のガバナンスにも有効であり、メカニズムを適切に組み合わせ個人の行動を制御しようとした。物理空間におけるアーキテクチャは、「壁で囲むこと」や「仕組みを車に組み込むこと」である行為が回避されるよう仕向けるが、サイバー空間のアーキテクチャは、「プログラムによる制御で機密情報を端末から発信できなくする」などプログラムの働きで同じ目的を達成する。レッシグは、サイバー空間におけるアーキテクチャとして重要なものは、プログラムやこれを構成する「コード」であるとした。

近年、こうした考えをブロックチェーンに応用した議論が展開されている。デ・フィリッピ (Primavera De Filippi) らは、ブロックチェーン上の規制対象は曖昧となっているとはいえ、利用者、マイナー、スマートコントラクト開発者、インフラ事業者など影響を及ぼしうる主体が存在し、立法などで直接に働きかけることも原理的に可能と指摘する²⁰。直接的な規制に加え、経済的なインセンティブ付与、規範の形成、アーキテクチャを構成するコードの策定過程への関与など多様な手法を駆使し、自律分散的なブロックチェーンに影響を及ぼしうるとした (BOX 図表)。

本文で言及した規制当局による様々な取り組みには、これらの議論と関連付けて解釈されうるものがある。本文中で取り上げたFSB報告書では、デ・フィリッピらの論考が引用されている。FATFでの議論は、サイバー空間における「法」や「規範」の形成を狙ったものと理解されうる。BGINでも、その目的に「信頼できる文書とコード」の策定を通じた学術的基盤の構築を含んでおり、アーキテクチャの重要な要素であるコードの策定に関与することで、ブロックチェーンにかかる実効性のあるガバナンスの提案を志向していることが窺える。

【BOX 図表】パブリック型ブロックチェーン影響を与えるメカニズム

メカニズム	具体例
法 (立法により直接的に禁止する)	・インターネットサービスプロバイダー、ウォレットサービスなどを規制。 ・検索エンジン、SNS、アプリのプラットフォームなどを提供する業者に働きかけ。
市場 (経済合理性に訴える)	・マイナーへのインセンティブ付与。 ・ブロックチェーンのコスト構造に影響を与える。 ・政府が市場に参加する（マイニングや暗号資産の売買など）。
規範 (望ましい規範の形成を促す)	・コミュニティの中で形成される規範が、社会にとって望ましいものとなるよう働きかける。
アーキテクチャ (コード策定などに関与する)	・コードやプロトコル策定の過程に関与し、望ましいルールを埋め込む。

(出所) De Filippi, P., and Wright, A., *Blockchain and the Law: The Rule of Code* などをもとに作成

¹ パブリック型ブロックチェーンのなかでも、特にイーサリアム上に構築される。

² スマートコントラクトという用語は、「自動化された手段を用いて契約を強制的に執行する仕組み」の意味で以前から使われてきたが、近年、パブリック型のブロックチェーンと結び付けられて、改めて関心を集めている。

³ これには最近の暗号資産の価格高騰も影響しているが、分散型金融で取引される代表的な暗号資産イーサの量でも、本年3月時点の規模が昨年対比で急拡大している。

⁴ TVLについては「ある分散型金融サービスに暗号資産を預け、得たトークンを更に別のサービスに預けた場合、両方も計上される」との指摘がある。

⁵ 以下で紹介する仕組みは、執筆時点で各サービスのウェブサイトで確認できた情報を元にしている。

⁶ DEX の設計や特徴については、以下の論文の補論4が詳しい。田中修一・副島豊、「分散型台帳技術による証券バリューチェーン構築の試み—セキュリティトークンを巡る主要国の動向—」、日本銀行調査論文、2020年

⁷ マーケットメイカー機能が自動運用されるDEXを、AMM (Automated Market Maker) と称することもある。

⁸ 実際には、流動性トークンを使えなくする (burn する) ことで、Uniswap から返済を受ける。

⁹ イーサリアム上のトークン発行の規格に則って発行されたトークンであることが要件である。

¹⁰ Compound に暗号資産を預け入れなくても、cToken をDEXで入手することで、Compoundでの借り手になれる。

¹¹ 計算資源を供給して報酬としてビットコインなどの暗号資産を得る行為をマイニングと呼ぶことを踏まえ、流動性を供給してトークンを得る行為を「流動性マイニング」と呼ぶことがある。なお、流動性マイニングとイーールドファーマーミングという用語については、どちらも「分散型金融サービスを組み合わせて利用し、収益を得る行動」という意味で、区別せずに使う事例もみられる。

¹² Financial Stability Board, “Decentralised financial technologies; Report on financial stability, regulatory and governance implication,” 2019.

¹³ FSB では、分散型金融技術を「1つ以上の仲介者や中央集権化されたプロセスの必要性を低減または排除する可能性のある技術」と定義している。

¹⁴ Schär, F., “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,” Federal Reserve Bank of St. Louis, 2021.

¹⁵ Schär, F. 前掲論考

¹⁶ Financial Action Task Force on Money Laundering, “Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers,” 2021.

¹⁷ こうした試みのひとつにセキュリティトークンがある (詳細は田中・副島前掲論文を参照)。セキュリティトークンに関する業界の最近の取り組みについては、日本銀行決済機構局開催の「決済の未来フォーラム セキュリティトークン分科会」(2020年12月)の議事概要資料を参照。

¹⁸ 日経フィナンシャル「『分散型台帳』が創る金融新秩序規制も共創時代」(2020年10月10日付)

¹⁹ Lessig, L., *Code: And Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006.

²⁰ De Filippi, P., and Wright, A., *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.

日銀レビュー・シリーズは、最近の金融経済の話題を、金融経済に関心を有する幅広い読者層を対象として、平易かつ簡潔に解説するために、日本銀行が編集・発行しているものです。ただし、レポートで示された意見は執筆者に属し、必ずしも日本銀行の見解を示すものではありません。

内容に関するご質問等に関しましては、日本銀行決済機構局 FinTech センター (代表 03-3279-1111) までお知らせ下さい。なお、日銀レビュー・シリーズおよび日本銀行ワーキングペーパー・シリーズは、<https://www.boj.or.jp> で入手できます。