



DeFi（分散型金融）の 現状と課題

志波 和幸

公益財団法人 国際通貨研究所 経済調査部 主任研究員

1. はじめに

ここ数ヶ月の暗号資産（仮想通貨）市場は活況を呈している。暗号資産に関する大手総合サイトのCoinMarketCap⁽¹⁾によると、12月17日時点で暗号資産は8,000種類以上発行され、その時価総額は6,130億ドル（約64兆円）と、9月末からの約2ヶ月間で2倍近く急増した。暗号資産の雄であるビットコインが史上最高値を更新したこともあり、最近では2017年末から2018年初にかけての「暗号資産ブーム」が再び到来した旨の記事を見かけるようになった。

その要因の一つとして、昨今の新型コロナウイルス対策の一環として世界的に金融緩和状態が長期間続く見込みが大きくなった結果、投資家が運用を求め暗号資産をはじめとするより高リスクの金融商品に注目したことが挙げられる。また、大規模な財政出動が講じられたことで世界全体の公的債務水準（対GDP比）は第二次世界大戦後のピークをも上回り過去最高に達した結果、将来の債務の持続可能性を不安視する投資家がインフレヘッジ目的⁽²⁾でビットコインを始めとする暗号資産を購入したためともいわれている。

しかしこのコロナ禍の影響とは別に、DeFi銘柄と呼ばれる暗号資産がその市場高騰を牽引していることにも注目すべきである。本稿では、DeFiの基本的な概念について説明するとともに、その可能性と課題について述べる。

2. DeFiとは

DeFiはDecentralized Financeの略語で、わが国では「分散型金融」と訳されることが多い。それは「ブロックチェーンのネットワーク上に構築される金融サービスまたはそのシステム」であり、換言すると、銀行や証券取引所や貸金サービスなどが提供する既存の「管理者が存在する」金融サービス⁽³⁾を、ブロックチェーンをはじめとする新たな技術を用いて「非中央集権型」のサービスに転換し、利便性や透明性がより高いものを提供することを指す。（図表1参照）

お互いに知り合いではない二者がモノやサービスのやり取りを円滑に行うためには、概して「モノやサービスの提供を着実に提供する／その代金を確実に支払う」という信頼を担保するモノやヒトや組織を介在させることを必要とする。現行の金融取引においては、

図表1 既存の金融システムとDeFiとの比較表

主な違い	既存の金融システム	DeFi（分散型金融）
取引の透明性	管理者本人及び管理者が許可した人のみ取引の閲覧・検証が可能	ブロックチェーン上に記録される取引は誰でも閲覧・検証が可能
システムの運用管理方法	金融機関等の中央集権者が運用管理する	運用管理の主体がない（プログラムまたはそれで稼働しているシステム自体を信用する）
利用者の資産管理方法	金融機関等の中央集権者に資産を預ける	ブロックチェーン上にて利用者自ら資産を管理する
システムの参加制限の有無	金融機関等の中央集権者が各人の参加可否を決めることができる	インターネットに繋がって、暗号資産を有していれば世界中誰でも利用可能
耐改ざん性	ハッカー等による取引データ書き換え防止策を講じる（追加コスト要）	ブロックチェーンの特性上、第三者が恣意的な理由で取引を無効化・改ざんできない

（各種資料より筆者作成）

国内外送金や貸金業務において銀行が、株式や債券の売買業務において証券会社はその役割を担い、中央集権者として法人や個人の顧客を仲介し取引円滑化を図っている。

しかし、これらの金融機関は競合他社に負けないよう質の高いサービスを提供し続ける必要がある結果、人件費やシステム運用費などの運営コストが恒常的に発生する。そして、それを顧客は手数料との名目で、たとえ該当するサービスをフルに享受していなくても、支払う形で負担している。

また、それら既存の金融サービスは管理者が存在するため制約がかかることもある。例えば、管理者サイドの都合によりそのサービスの提供時間を制限することがある。また、取引に関する各種手数料は原則管理者が決定し、利用者はその決められた手数料体系に則り支払わなければならない。加えて、管理者が営業拠点にしている国が制定する法律・規則・ガイドラインを遵守するべく、それらに基づき利用者の参加や取引を制限することもある。

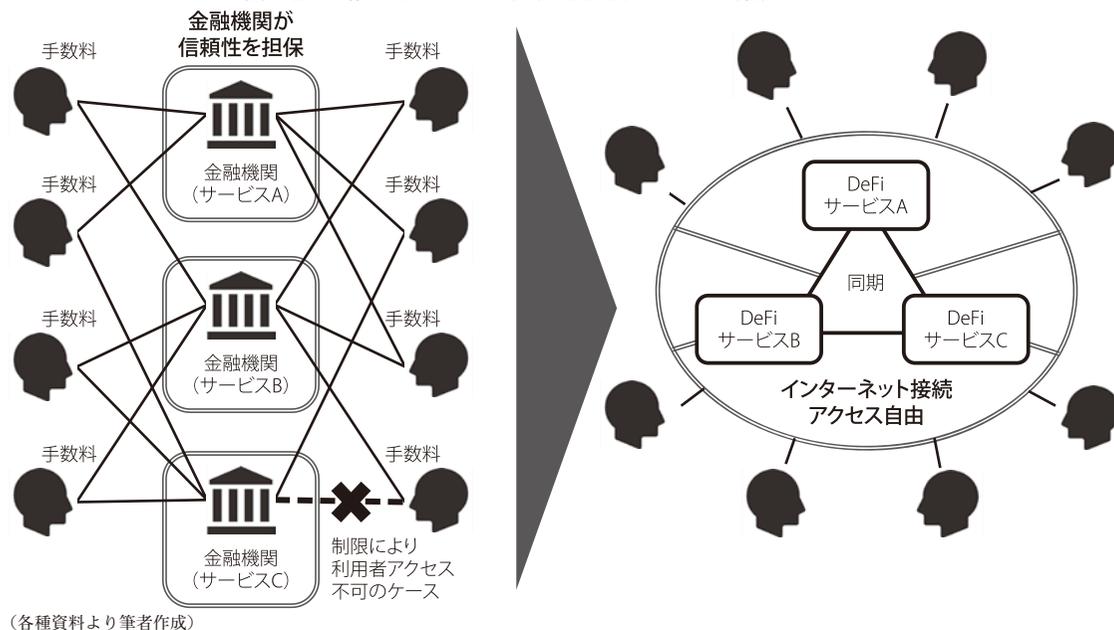
これに対し、DeFi は特定の条件に合致した場合にのみ自動的に取引を実行するようあらかじめプログラミングされており（これを「スマートコントラクト」という）、運用開始以降は管理者が不在とするシステム構成であるた

め、いつでも（24時間／365日運用が可能）どこでも（国境を越えて）利用者が自由にアクセスできるサービスを提供できる可能性を秘めている。さらに、DeFi は中央集権的に運用管理するためのファシリティや人員を必要とせず、初期コストもランニングコストも抑えることができると言われ、結果従来のシステムよりも利用者に課せられる手数料がはるかに安価となることが期待されている。加えて、その手数料体系も、需給に応じリアルタイムに変動するなど自由にカスタマイズすることが可能である。

また、「スマートコントラクト」に同期することで、提携やAPI 開発など異なる金融サービス間の連携の際に必要な作業を極力少なくすることが期待されている。このようにDeFi を活用して金融サービスを重層的に構築することを「Composability（構成可能性）」や「BaaS：Banking as a Service」と呼ぶが、それがあたかもおもちゃのブロックを積み重ねて新たなカタチを作り上げる行動に似ていることから、世界的に著名な玩具会社 The LEGO Group の玩具の一つである「レゴブロック」を用いて説明されることもある。（図表2 参照）

これらのメリットを有する DeFi は、従来で

図表 2 既存金融サービス（左）と DeFi サービス（右）のイメージ



は不可能であった新たな金融サービスの提供や、既存よりもはるかに便利なサービスの構築が期待されている。

3. DeFi の市場規模

DeFi に関する総合サイト DEFI PULSE⁽⁴⁾によると、執筆時点でそのサービス数は 160 以上あり、市場規模を示す指標のひとつである TVL (Total Value Locked: 各サービス・システムで稼働しているスマートコントラクトにロック (取引条件を満たし執行されるまで一時的にプール) されている暗号資産の時価総額) は 2020 年 7 月から急増し、約 156 億ドル (約 1.6 兆円) に達した。(図表 3 参照)

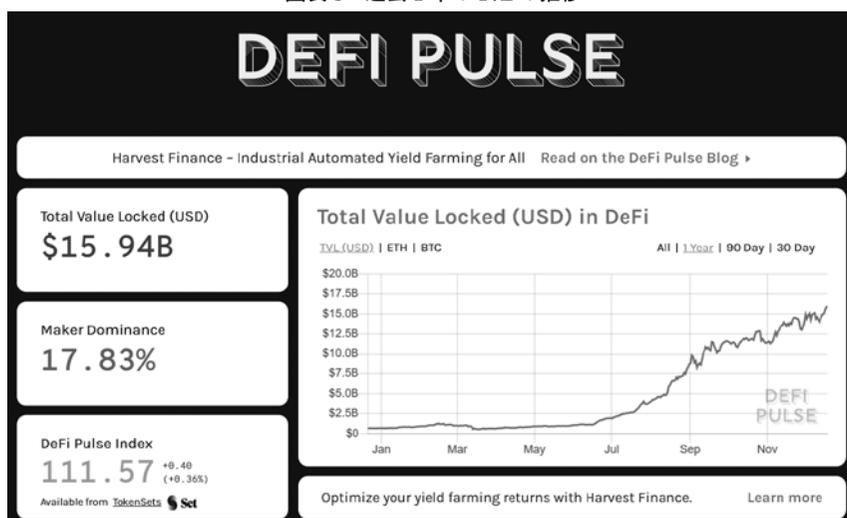
DeFi の活用が期待されている領域は、「レンディング業務」、「暗号資産取引所」、「デリ

バティブ」、「市場予測」等多岐にわたる (図表 4 参照)。紙面の都合上、以下では代表的な領域である「レンディング業務」の概要を説明したい。

レンディングとは、取引所等のプラットフォームに暗号資産 (仮に「A」とする) を担保として預け、①それを貸し出して利息収入を得るとともに、②担保を元手に別の暗号資産 (仮に「B」とする) を借りる行為を指す。これにより、担保として暗号資産 A を供与した投資家は、それを売却 (利益確定) することなく、さらに値上がり期待される (と判断した) 暗号資産 B を購入する、いわゆるレバレッジを掛けた投資が可能となる。

Compound (コンパウンド) は、2018 年 9 月にレンディングサービスの提供を開始した大手プラットフォームであるが、その大まか

図表 3 過去 1 年の TVL の推移



(出典) DEFI PULSE

図表 4 DeFi の活用が期待されている主な領域

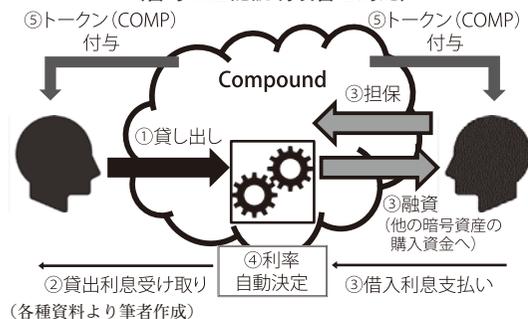
領域	概要	代表的な金融サービス名
1 レンディング業務	保有する暗号資産を貸し出し、その額に応じた報酬(利息・配当)の獲得を目指す。また、貸出額を担保に別の暗号資産に投資する。	Compound、MakerDAO、Arve
2 暗号資産取引所	DEX (Decentralized EXchange: 分散型取引所) と呼ばれる。資産をいったん預ける必要もなく、板取引も不要。	Uniswap、Sushiswap、Curve Finance
3 デリバティブ	取引所を bypass せず、暗号資産のレバレッジ取引を実施 (ロング/ショートいずれも可能)。	EXPO
4 市場予測	「ある専門家による意見」ではなく、「個々の決断による意見」を集約し未来の市場動向を予測するもの。	Augur
5 ステープルコイン	価格変動が相対的に小さいステーブルコインの流動性供給サービス。貸し出し額に応じた報酬 (利息・配当) の獲得が期待される。	Curve
6 KYC	DeFi システムの一連のスマートコントラクト全体を監査するシステム。	ConsenSys
7 DeFi 取り纏めサービス	DeFi サービスを1つのアプリで利用できるようにするサービス。複数の競合サービスがある場合は、利用者にとって有利なサービスに自動誘導するものもあり。	InstaDApp

(各種資料より筆者作成)

な事務の流れは以下の通りである。(図表5参照)

- ① 投資家が暗号資産(仮にその名称が「Token」とする)を預けると、その見返りとして「cToken」というCompoundが発行するトークンを受け取る。この「cToken」は、多数の投資家が預けたTokenをプール(一時保管)した内の個人の持分を表したものであり、それを提示すればいつでもTokenに交換が可能である。
- ② 投資家はCompoundに預けた暗号資産を貸し出すことにより、その貸出利息等の収入を得ることができる。
- ③ 一方、投資家はCompoundに預けた暗号資産のその時点の時価の上限(暗号資産毎に50%から75%の範囲内で設定)まで「担保付き融資」を受けることができる。そしてそこで借り入れた分を別の暗号資産購入に用いることができる。
- ④ ②の「貸出利率」と③の「借入利率」は、その時の需給状況によりリアルタイムで変動するようあらかじめプログラミングされている。つまり、暗号資産を借りたいという需要が大きく(小さく)なれば、貸出金利は高く(低く)なり、その水準は管理者や投資家が恣意的に決めることができない。
- ⑤ なお、当該サービスを利用した投資家に対しては、あらかじめ決められたルールに基づき、今後のCompoundの(バージョンアップ等の)意思決定に対して投票できる権利を有するトークン(COMP)を付与する。COMPのような投票権を有するものを「ガバナンストークン」と呼び、その一部は取引所等で売買することが可能である。

図表5 Compoundの事務フロー
(番号は上記説明項番と対比)



これまで多くの投資家は、取引所に暗号資産を預けたまま何もせずに放置するほかなかった。そこでCompoundが暗号資産の貸し出し機能や担保付き融資機能を簡単な操作で行うことができるサービスを提供したことから、人気を博して利用が急増。直近のTVLは17億ドル(約1,760億円)と半年前と比べ3倍になったうえ、参加者に付与しているトークン(COMP)の時価総額も6.8億ドル(約700億円)に達している⁽⁵⁾。

4. DeFiの課題(ICOの二の舞となるのか)

暗号資産を用いた新たなサービスの提供の動きは過去にも存在した。その代表として挙げられるのはICO(=Initial Coin Offering)である。

2017年に発生したICOブームでは、将来性があり有望そうに思えるプロジェクトの発起人がホワイトペーパー(事業計画書)を作成・公開し、独自のトークンを発行・販売して投資家から資金調達を行った。そして独自に発行したトークンを各国の暗号資産取引所に上場し、投資家がそれを売却することでキャピタルゲインを得るという仕組みになっていた。それにより、数々のICOが数億円単位での資金調達に成功し、それで発行・販売されたトークンがブームにも乗り次々と高騰していった。

しかし、ICOには「ホワイトペーパー」というインターネット上で公開された計画書のみで、投資家はそのプロジェクトが成功するかどうかを判断しなくてはならないという弱点があった。例えば、わが国で株式を新規上場するには「形式要件(企業の継続性、財政状態、収益力等の面からの上場適格性を保持するための要件や、適正な企業内容の開示を確保するための要件等)」と「実質審査基準(企業経営の健全性、企業のコーポレート・ガバナンス及び内部管理体制の有効性等)」を満たしているかどうかを取引所が事前に審査する必要がある。それに対し、「ホワイトペーパー」には公表するための法的要件はなく、それがため具体的なプロジェクトやサービス

がない状態であるにもかかわらず、より将来性があるように“みせかけた”プロジェクトを立ち上げ、それに魅せられた投資家から多額の資金が投入された。そしてそれら乱立したプロジェクトの殆どがなんの成果を上げることなく終了した結果、多くの ICO コインは暴落し、ほぼ無価値になってしまった⁽⁶⁾。

このような ICO ブームの狂乱と比べると、DeFi にはプロダクトやサービスが既に存在し、その実用性を判断しつつ投資家からの資金を集めているという大きな違いがあり、ICO よりも実体性を有していることが DeFi の強みともいえる。

しかし、依然として以下のようなリスクが潜在していることに注意が必要である。

①ハッキングリスク

スマートコントラクトは、ルールが一度プログラミングされ運用開始されると、そのルールの途中変更は原則不可能である。そのため、運用開始前に開発者は様々な事態を想定しシミュレートしているのであるが、それでもバグは発生し、かつそれが永久的に解消されないこともある。

また、DeFi サービスのなかには、昨今の DeFi ブームに乗り遅れまいとシステム開発を急ぎ、すべての必要な検証を通過せずにリリースしたものもあると言われている。その結果、ハッカーがそのデザインの弱点と欠陥に気づき、資金の盗用事件が頻発している。(図表 6 参照)

この動きを裏付けるようなデータが暗号資産分析企業であるサイファートレース社 (CipherTrace) から出ている。2020 年 11 月

10 日に同社が発表したレポート⁽⁷⁾によると、暗号資産の盗難やハッキング、詐欺による被害額の合計が、2019 年の 44 億ドルから 2020 年 (1 月から 10 月まで) は 18 億ドルと大幅に減少したものの、DeFi 分野でのハッキング事件が 2019 年には「ほとんど無視できるもの」だったが、現在では全体の 20% を占め、著しく増加していることを指摘した。そして、「DeFi の急成長は、最終的にハッカーを引き付けることになり、このセクターで多くのハッキングをもたらした」と警告している。

②スキーム (詐欺) 事案の増加

DeFi 市場が注目されるにつれ、ICO ほどではないにせよ詐欺的なプロジェクトが増加することが予想される。

元来 DeFi のプログラム・コードはオープン (公開) のため、簡単にそのコピー版を作成することが可能である。最近では yearn.finance (複数のレンディングサービスのなかから、投資家にとって最も高い貸出利率を提供しているサービスをリアルタイムで提示し、資金を自動振替するサービス) のコードをコピーした詐欺プロジェクトが複数見つかっている。

それ以外にも、有名な DeFi サービスのホームページを偽装し (フィッシングサイト)、投資家の個人情報及び保有暗号資産を盗む等の事件も発生している。

③「ガバナンスの分散化」は正義なのか？

DeFi サービスは運用開始当初から管理者がいないわけではない。前述の Compound をはじめとする多くのそのサービスは、一定期間運用後に利用者へ (バージョンアップ等の)

図表 6 2020 年 4 月以降発生した主な DeFi サービスのハッキング被害

	発生年月	DeFi サービス名	被害内容 (公表額)
1	2020 年 4 月	d Force	2,400 万ドル (約 25 億円)
2	2020 年 4 月	Lendf.ME	2,500 万ドル (約 26 億円) 以上
3	2020 年 6 月	Balancer	50 万ドル (約 5,200 万円)
4	2020 年 9 月	Eminence	1,500 万ドル (約 16 億円) (その後ハッカーが 800 万ドル返還 (理由不明))
5	2020 年 10 月	Harvest Finance	2,400 万ドル (約 25 億円)
6	2020 年 11 月	Origin Protocol	700 万ドル (約 7 億円)
7	2020 年 11 月	Akropolis	200 万ドル (約 2 億円)
8	2020 年 11 月	Value DeFi	740 万ドル (約 8 億円)
9	2020 年 11 月	Pickle Finance	2,000 万ドル (約 21 億円)

(各種資料より筆者作成、1 ドル = 104 円で換算)

意思決定に対して投票できる権利を有するガバナンストークンを付与することで、中長期的にその決定プロセスを委譲することとしている。

しかし、その分散化の過程で、大口利用者による投票乗っ取りのリスクや、投票者数が多すぎる（小口化しすぎる）ことによる意思決定の鈍化やバグ対応の遅延などの新たなリスクが発生することが懸念されている。

④ トークンの価値の妥当性

前述の通り、DeFi サービスの多くは、利用者による意思決定に対して投票できるガバナンストークンを付与する。そして、そのトークンは取引所等で売買が可能である。

しかし、その金融サービスが実態をもっているとはいえ、現在のトークンの価値がそのサービスの実態を正しく反映しているとは限らない。つまり、現在暗号資産市場全体が高騰しているなか、「買うから上がる／上がるから買う」という投資家心理が過度に価格に上乘せられている可能性がある。

5. 各国当局の動き

かような DeFi 市場の拡大を受け、2019 年 6 月に金融安定理事会（FSB）が分散化金融技術に関する報告書⁽⁶⁾を公表し、金融システムの分散化はその競争の拡大と多様性をもたらす可能性がある一方、主要なインフラや技術の所有権や運営の問題、法的責任の曖昧さ、消費者保護に関する不確実性等の課題を指摘した。そして、付属書 2（管理者の許可が不要な（パーミッションレス）分散台帳に関するガバナンスの問題点の明確化）で、そのシステムの潜在的なガバナンスリスクとして、①システムの変更・更新管理体制の脆弱さ、②関係者間の意見の相違発生を起因とする複製システムの出現・増殖の恐れ、③利用者のプライバシー保護と取引の可視性とのバランスのとりの難しさ、の 3 点を挙げた。

当該報告書の公表後も、わが国をはじめ各国の金融規制当局は DeFi に対し明確な規制の枠組みを定めず、静観の姿勢を貫いている。

しかし今後 DeFi 市場がさらに巨大化するとともに、重大なセキュリティ事件が発生したり発生する懸念が増したりすると、当局は規制制定の方向に向かっていくであろう。その時、「管理者の分散化」や「Composability」などの DeFi の特徴が規制により損なわれる恐れがある。

6. おわりに

上記の通り、DeFi の存在が知られ始めてきているが、そのサービスは総じて黎明期にあり、今後それらが既存金融サービスを凌駕するものになるかどうかの予測は難しい。むしろ、DeFi システムはまだ不完全な部分があり、ハッキングなど不正流出被害が多数発生する等、負の面が明らかになってきた。前述のサイファートレース社も、DeFi には顧客の本人確認（KYC）のようなプロセスがない場合がほとんどであるため、DeFi 業界が「マネー・ロンダラーの天国」になっていると指摘している。

昨今の暗号資産市場の過熱とともに今後も様々な DeFi サービスが登場するであろうが、投資家・利用者は既存金融サービス以上の十分な事前調査及び冷静な判断が求められる。

《注》

- (1) <https://coinmarketcap.com/> をご参照。
- (2) インフレに強い資産の代表に金（ゴールド）が挙げられるが、その有限性等の同様の特徴をもつ暗号資産が「デジタル・ゴールド」として注目されているといわれている。
- (3) DeFi に対し、国内外送金には銀行が、株取引には証券会社が等、中央集権機構（管理者）が存在する金融サービスを CeFi（Centralized Finance）と呼ぶこともある。
- (4) <https://defipulse.com/> をご参照。
- (5) この時価総額は、暗号資産約 8,000 種類のなかで 40 位前後の規模である。
- (6) 一連の流れの詳細は、国際金融 1319 号（2019 年 4 月 1 日発行）掲載の拙稿「仮想通貨取引のマネーロンダリング対策の現状～過渡期にある仮想通貨市場を踏まえ～」をご参照頂きたい。
- (7) Crypto crime slows in 2020, but 'DeFi' hacks rise - CipherTrace report (2020.11.20, Reuter 提供) をご参照
- (8) "Decentralised Financial Technologies" Report on financial stability, regulatory and governance implications" (June 6th, 2019 FSB) をご参照