

パブリックプロトコルとDAOがもたらす新しい未来の社会

鈴木 雄大 ●Fracton Ventures株式会社 共同創業者

注目が集まる分散型金融アプリケーションのDeFi。パブリックプロトコルとして成長を続け、UI、UX分野にも影響を広げた。2021年はさらなるプロトコルの出現、DAO化の加速に期待。

■2020年のブロックチェーン業界におけるムーブメント

2020年版のインターネット白書に寄稿してから、既に1年が経っている。2021年版も幸いなくとにブロックチェーン分野で執筆させていただくことになったが、この1年は振りかえってみても驚くほどに速く過ぎたように感じる。2020年が激動の年だったことは言うまでもないだろう。その中でパブリックブロックチェーンを取り巻く環境においては新しい可能性を感じる出来事が複数登場していたと言えるのではないだろうか。

メディアでもブームとして特に大きく注目されたのは、2020年版でも紹介したDeFi（ディーファイ）と呼ばれる分散型金融領域の成長だ。DeFiの定義はいくつかあろうが、ここでは「十分にネットワークの管理が分散されたパブリックブロックチェーン上にスマートコントラクトを核として動作するプロトコル」、また「そのプロトコルを元にサービスUIを追加した分散型金融サービス」を指すと定義させていただく。

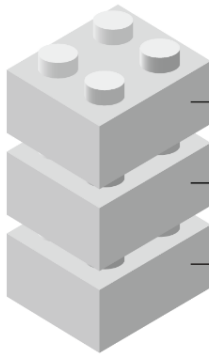
分散型アプリケーションとしては以前からDapps（ダップス）という用語が用いられている。DeFiはDappsの一つのジャンルであり、金融領域のDapps群を総称する言葉として利用され

ている。ただ2018～2019年にDappsと呼ばれたプロダクトの多くは、パブリックブロックチェーン上のスマートコントラクトにてアプリケーション上の挙動全てが記述されることはなく、スマートコントラクトを用いた部分と、そうではないオフチェーンと呼ばれる既存のデータベースシステムを用いながら、例えばゲームにおける売買用のアイテムなど必要最低限の一定の情報だけをパブリックブロックチェーンに記録するという手段を取っていた。

これに対して、DeFiのスマートコントラクトであるプロトコルと呼ばれている箇所ではアプローチが異なる。DeFiプロトコルは原則スマートコントラクト単体で完全に金融サービスを提供している。これらをパブリックプロトコルと呼ぶことができる。これらは言うならば公共性を持ったプロトコルであり、段階的な分散化の道を歩むことで原則コミュニティとなる利用者からなるトークンホルダーに権限を譲渡し、それにより改善・開発がなされている。

パブリックプロトコルの御三家とも呼ぶべきプロトコルを紹介しよう。①ステーブルコインの発行を行うことができるMakerDAO（メーカーダオ）②暗号資産同士の貸し借りを自動化した

- ・ Decentralized Finance = 分散型金融
- ・ ネットワークの管理が分散されたパブリックブロックチェーン上にスマートコントラクトを核として動作するプロトコル、またそのプロトコルを元にサービスUIを追加した分散型金融サービス



User Interface

- ・ 一般的に操作が可能となる操作画面 (Website)

Smart Contract

- ・ 全自動で特定の動作を行うコード

Public Blockchain

- ・ ノードが分散されたパブリックブロックチェーン

出典：Fracton Ventures

Compound (コンパウンド) ③ AMMという自動価格決定のメカニズムを内包することで即時に暗号資産同士をブロックチェーン上で交換することを可能にしたUniswap (ユニスワップ) である。

■パブリックプロトコル、Uniswap

2020年版に寄稿した記事でMakerDAOの例は既に挙げているので、ここではUniswapの例を挙げる。Uniswapのコンセプトはブロックチェーン上で即時トークンを交換できる暗号資産取引所、いわば分散型取引所のシステムだ。Uniswap以前もトークン交換を完全にブロックチェーン上で行おうとしたプロジェクトは多かったが、その多くで売買の板を設けながらリアルタイムの売買情報を完全にパブリックブロックチェーン上に乗せることには実質不可能になっていた。これはEthereumブロックチェーンが1ブロック生成間隔に約15秒かかっていることなどが要因である。事実、分散型取引所モデルとして先行したdYdXなどは一部をあえてブロックチェーン外で処理を

することで顧客の求める速度を実装した。

それに対してUniswapは全く異なるアプローチを行った。Automated Market Makers (AMM)と呼ばれるシステムを採用した。AMMは一部の顧客から自身の保有トークンをプールなるスマートコントラクト上の貯蔵タンクにロックさせることで、AMMへの流動性を供給するという役目を負ってもらうことで成り立つ仕組みである。この流動性を提供されたトークンを売買の約定用に使用している。これにより売買の相手方を一切不要にしながらも、即時トークンの交換を行うことができる。

またUniswapプロトコルは、ドキュメントページにも書かれているように、オープンソースによりソースコードも包み隠さず公開されている。これは既に一種の公共財と言えるものであり、利用手数料や他のトークンをUniswapプロトコル上に追加する手数料すら完全に無料である。この戦略は従来の暗号資産取引所では絶対に成り立たなかったモデルと言えるだろう。

なおUniswapに関しては開発を行ったユニバー

サル・ナビゲーションが存在しているが、スマートコントラクトにおける変更権限などは極限まで省略していることが認められており、同社が実質的に開発を担ったことは事実であるものの、方針としてコミュニティ主導のガバナンスに移行しようとしている。

ちなみに Uniswap の開発までを支えた資金はベンチャーキャピタルによるリスクマネーであり、アンドリーセン・ホロウィッツ (a16z) などのシリコンバレーを代表するベンチャーキャピタルがその成長性と企業ビジョンに共感し投資を行っている。現に同社は Uniswap プロダクトで後述する UNI トークンの同社への配布分を除き、Uniswap プロトコルからは一銭の売上も上げていないまま、わずか 10 人以下という少人数でプロダクトを磨き上げることが可能であった。

話を戻そう。プロトコルが真の意味で分散型になるには、運営を開発企業から利用者・開発者のコミュニティへと譲渡していく、段階的分散化と呼ばれるプロセスを踏む必要がある。これが DAO (ダオ) 化である。DAO は Decentralized Autonomous Organization の略語であり、自立分散型組織と訳すことが可能である。なぜ DAO 化が重要なのかというと、そのスマートコントラクトが企業の 1 プロダクトから 1 つの公共財になるかどうかが変化するポイントだからだ。

この公共財になる DAO 化プロセスで重要になってくるものがガバナンストークンである。ガバナンストークンはプロトコルへの提案・投票権だけを付与したユーティリティトークンであり、このトークンを誰に保有してもらうかという観点からプロトコルをコミュニティへ権限譲渡していくプロセスにおける、一つの重要なファクターになっている。

例に挙げている Uniswap であれば、2020 年 9 月 16 日に公開されたブログにおいてその独特な

配布方法が注目された。Uniswap のガバナンストークンである UNI トークンを初期に手に入れることのできる方法として、過去 Uniswap v1、v2 を利用したことのあるウォレットアドレス最大 1 万 2000 に 400 UNI が自動的に付与される決定がなされた。その他流動性提供を行ったことのあるウォレットアドレスにはさらにプラスのインセンティブとして少し多くの UNI が受け取れるようになっていた。

このように過去のユーザーに対してインセンティブを与えた方法は遡及的配布などと呼ばれており、初期からプロトコルを利用したユーザーをブロックチェーン上で特定して確実に付与が行える観点から、パブリックブロックチェーンの特性を最大限活かした方法と言える。またアーリーアダプターのユーザーを可視化する一つの方法でもあるとも言える。

■ UI/UX 改善による裾野の広がり

DeFi 分野の成長により、大きく成長した分野が Dapps 領域における UI (ユーザーインターフェース)、UX (ユーザーエクスペリエンス) である。そもそもパブリックブロックチェーン領域では以前から UI、UX 分野よりも技術的に複雑なことを行う方に意識を持つ開発者が多く、一定のリテラシーがないと利用できないような画面操作となっているものが多く、結果的に新規参入ユーザーを妨げる一種のハードルとなっていた。しかしながらこの DeFi のムーブメントは、UI、UX 分野においても大きな変化をもたらした。

例えば Uniswap のプロトコルをフォーク (コードのコピー) し、独自トークンを利用者に付与するという差異だけを持って生まれた競合プロトコル SushiSwap (スシスワップ) の誕生が挙げられるだろう。非常にわかりやすい、一種金融というよりもゲームのような UI を採用することで、誰

でも気軽にプロトコルを用いられるという体験をもたらした。誰でも利用可能なわかりやすいデザインによるUIがウケたことで利用者が増大するきっかけとなったのは言うまでもないだろう。

この流れはプロトコルだけではなく周辺サービスにも及んだ。秘密鍵を利用者個人が管理するウォレットサービスである英国のスタートアップが提供する「Argent Wallet」は、UI、UXを追求した新しいタイプのウォレットサービスであり、秘密鍵を完全にユーザー本人が管理することをリテラシーの高さの有無に関係なく行えるよう、裏側で専用のスマートコントラクトが自動生成されているコントラクトウォレットと呼ばれる仕組みを採用している。

またArgent Walletにはソーシャル・リカバリーという機能が盛り込まれている。現実社会で信頼がおける人物をArgent Wallet上で登録しておくことにより、Argent Walletのログインに必要な情報を失いログインができなくなった際に、信頼できる人物からウォレットの復元というプロセスを行ってもらうことでウォレット機能を回復することができる。従前のウォレットサービスがシードフレーズと呼ばれる特定のランダムな英単語を順通りに覚えさせることで復元を可能にしていたことに比べると、ついに一般的なスマホアプリの延長線上で用いることができる暗号資産ウォレットアプリが登場したと言えるだろう。

■プロトコルを再活用する新サービス

今後注目されるパブリックブロックチェーン上のプロトコルを用いたサービスについて紹介しておく。例えば米国の物販用プラットフォームのスタートアップ、ZORA（ゾラ）は裏側に既存のDeFiプロトコルのロジックを使うことで全く新しい自社サービスとして展開する、いわばプロダクトオンプロトコルの設計に基づくサービス

「ZORA」を提供している。

仕組みを説明しよう。ZORAは一見すると単にセレクトショップのECサイトのようなプラットフォームである。同社がセレクトしたアイテムがデジタルで販売されているだけに思える。実際にZORAではナイキの希少価値の高いスニーカーなどが販売された。しかしながら販売されているものは実際の商品と引き換えられる個別の専用のトークンであり、そのトークンはUniswapのプロトコルを用いた自動的な価格決定により販売がなされている。

さらに詳細な説明をすると、ユーザーはステープルコインというドルに価値がpegされたトークンまたはクレジットカードを用いて、ZORAのウェブサイト上からトークン化された商品を購入することができる。この際裏側では購入金額と同額がzUSDCというZORA内専用のトークンに交換された上で、ZORA側からUniswapのプールに対して売買のトランザクションを実行している。

つまりZORAでは裏側にUniswapのプロトコルをそのまま活用することで、トークン化されたアイテムを細かい単位で販売する際にも完全に自動的な価格決定が行えるという利点を活用しながら、ZORAのウェブサイト上からのみアクセスを可能にするというロジックを活用している。これによって比較的速い自社プロダクト開発を可能にした。

このように公共財のプロトコルを活用することで、フルスタックで開発する手間を省きつつ、常に新しいプロトコルの仕組みを最大限活用したプロダクトを開発することができる。これは確実にイノベーションであろう。プロダクトを出すまでに必要な開発者の人数も、その人件費も圧倒的に抑えながら開発を行うことができる。この恩恵は全てプロトコルが公共財として成立していることと、そのソースコードが全てGitHubなどで

オープンソース形式として公開されていることによる。

■ DAO化の加速

2021年のパブリックブロックチェーン、ブロックテクノロジーに期待する箇所はサステナビリティであろう。公共財化してくるプロトコルが成り立ち得るという事実を証明した2020年を経て、それらプロトコルの継続的な開発・改善提案を、ガバナンストークンを持つコミュニティがリードして行っていくか、またそれが短期的なブームになることなく継続して行えるかであろうと考える。

またDeFiで見られたインセンティブ設計を活用した「利己的に働くことで成立するバランスの取れた設計」は単に金融からスタートしたもの、他の分野にも応用できる仕組みであろう。興味深い点として、金銭的インセンティブの付与はドライにユーザーに何かを行わせるトリガーにのみなり得るが、その一方でコミュニティ上ではすぐに金銭的リターンが出ない提案や長期的な視点で見た際に必要となる機能の開発などが行われている。こうした渦にも似たコミュニティの盛り上

がり、ブロックチェーンのコミュニティが世界規模の優れた開発者を虜にする魅力を持っており、どんなに大金を払っても雇えないような優れた開発者や広く社会のことを考えるアントレプレナーシップを持つ経営者が続々と参画してくる現象が起きている要因でもある。

また2020年は多くのDeFiをはじめとするDappsの基盤となるEthereumブロックチェーンにおいて次世代型のEthereum 2.0へと移行を行っていくための第1弾プロセスであるPhase 0が開始された。プロトコルなどの上位層でのニーズに応じていくためにも、インフラストラクチャとしてのブロックチェーン基盤のアップグレードが急がれている。

上記ブロックチェーン自体のアップグレードを含め、2021年にはさらなるプロトコルの出現、そしてDAO化の加速が行われることを期待せずにはいられない。確実に存在するこの価値を持つコミュニティは、そのネットワーク規模が拡大していくにつれて、さらに優秀な人々を巻き込み、やがて世界を持続可能な社会にしていくピースとなる未来をもたらすことを私は切に願っている。



1996, 1997, 1998, 1999, 2000, ...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2021年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp

©1996-2022 Impress R&D