ブロックチェーンの次世代環境と注目アプリケーション

鈴木 雄大 ●株式会社マネーパートナーズ 社長室

分散型金融アプリケーションDeFiがこの1年で拡大。合意形成メカニズムはPoWからPoSへと移り、レイヤー2の開発も進む。ブロックチェーンには実社会の課題解決が求められている。

■DAppsにおけるブームの終焉

昨年の2019年版で、私は当時ブームであったDApps（ダップス）について論じた。このときのDAppsは、ゲームや企業のサービスをブロックチェーン上に形成することを指していたにすぎない。執筆していた2018年頃はトークンエコノミーという言葉が独り歩きする程度にはそうした実験的試みへの期待が少なからず存在していたように思う。しかし、ブロックチェーンの世界において変化のスピードは桁違いに速い。よくブロックチェーン分野での時の流れは通常の3倍の速さであると冗談を言われるが、体感ではそれ以上であろうと私個人は思っている。

1年が経ち、DAppsは当時想定していたものとは少し違う形に進化したと考えている。実はこの文章を執筆している2019年末現在、ブロックチェーン業界内でDAppsという表現を聞かなくなっている。その理由は複数あると考えられる。

1つ目は、DAppsの定義である。昨年の寄稿の際、私はDAppsとは止まることのないプロトコルに由来するパブリックブロックチェーン上のアプリケーションであると定義した。しかし、そうした100％プロトコル形式での複雑なスマートコントラクトをベースにしたDAppsをビジネスで提供することはまだまだ難しい。サービスの将来性に鑑み、更新性を持つスマートコントラクトを記述することの難しさに加え、公開されると誰もがソースコードを確認できてしまうため、脆弱性攻撃を意識したパブリックブロックチェーン特有のコード監査を常に行わなければならない。このコストゆえ、企業の参入はなかなか進展しなかったと思われる。

2つ目は、日本国内では2020年に施行される暗号資産関連の法改正によりカストディ事業者にも仮想通貨交換業の規制が及ぶことが明確化された[1]ことである。これを嫌気したのか独自トークンを軸にしたプロトコル主体のサービスを行う会社はこの1年、ほぼ現れなかった。しかし一方で、独自の発展を遂げた分野もある。ゲーム領域を中心としたNFTである。NFTはNon Fungible Tokenの略で、絵画のように常に同じものが存在せず、代替性のないトークンを指す。Ethereum（イーサリアム）ではCryptoKittiesが採用したERC721が有名である。日本のスタートアップではこうしたNFTをゲーム内のアセットに紐付けるサービスが複数展開されている。代表的なものはdoublejump.tokyo社が提供するMy Crypto Heros（通称マイクリ）である。同社のNFTのス

マートコントラクトはトランザクション数でもNFTのものでは群を抜いており、国内1位の座を築いている。もともと日本ではソーシャルゲームの市場が大きかったこともあり、Ethereumのウォレットで対応できるNFTゲームはそれぞれ一定の成功を示したように思える。

一方海外市場においては、ゲームマーケットが伸びたという報告はあまり聞いていない。執筆時点では、トランザクション数でマイクリを超えるブロックチェーンベースのカードゲームであるGods Unchained Cardsなどは確かに生まれたものの、大きなムーブメントになる要素は少なかったように思われる。

では、海外で発展したのは何か。それはDeFi（ディファイ）と呼ばれる分散型金融の領域であろう。DeFiとはDecentralized Financeの略である。DeFiは、まったく新しい領域というわけではない。DAppsの1ジャンルである。

■DeFiムーブメント

DeFiが特に盛り上がっているのはEthereum上である。これは、MakerDAOという仕組みが大きく関係している。MakerDAOはDAI（ダイ）と呼ばれる1ドルに限りなく近い価値を1：1でペッグ（維持）したトークンを生成できるスマートコントラクトのシステムだ。通常ステーブルコインは現物の米ドルを担保に取ることが多く、Tether（テザー）社をはじめ、その運用コストやオペレーション、事業体の信頼性が何度も話題になってきた。DAIはそれらすべてをEthereumベースで作ることにより、スマートコントラクトでロックをかけることが可能なETH（イーサ）というアセットを担保にして生成される。このコントラクトをVault（ヴォルト、旧名称CDP）と呼ぶ。DAIはETHを担保にしたアセットであるため、DAIを自分の作成したVaultに戻すことでETHを償還できる。また償還を行わない場合には安定化手数料と呼ばれる手数料をDAIで支払うことで、DAIを持ち続けることが可能である。このために使用するMKRには手数料調整のための投票権が付与されており、これを行使することでトークンの価格が1ドルから乖離することを防ぐ仕組みとなっている。

DAIについて詳しく説明するのには大きな理由がある。DeFiはその多くのサービスがDAIを基軸に提供されているからである。具体例を挙げると、DAIを貸し出すサービス、DAIの金利分のみを先に別のトークンにして受け取ることのできるサービス、さらにそれを元にレバレッジ取引に近いものを提供するサービスなどがある。MakerDAO自身が提供するDai Saving Rate(DSR)という、DAIをスマートコントラクトにロックさせることで金利に近い概念のものを取得する方法も存在する。

このようにDeFiはDAppsのスマートコントラクト由来という特徴をいかし、パブリックブロックチェーン上であれば確実に透明性を持ってサービスを提供することで圧倒的に存在感を強めていった。驚くべきことであるが、750億円もの資金がすでにDeFi上にロックされている[2]。そのようなマーケットはブロックチェーン分野で未だかつて起きたことがなく、大変興味深い。

しかしDeFiはあまりに未成熟なマーケットだ。これほどのお金に相当する暗号資産をいくつかのスマートコントラクトだけでロックをかけている状態であり、このサービスのすべてが秘密鍵を預からない、原則的にはトークンそのものの移管ができないNon-custodialと呼ばれる方法で運営されている。つまり対検閲性は高いが、スマートコントラクトのバグに起因して資産が盗難されるなどのリスクは、現状それぞれのプロジェクトとサービスの利用者自身が負っている形である。

もちろんスマートコントラクトはオープンソースであるため、開発者であればソースコードを見ることは可能だ。しかしながら一般のユーザーがそこまで確認できるわけでもなく、まだまだリスクが拭えない状態が続いていると言える。すでにスマートコントラクトを対象にした保険サービスを提供する事業者が出始めているが、そのようなDeFiユーザーのリスクを軽減する仕組みがより身近な方法で利用できないと、アーリーアダプターを超えたレイトマジョリティー層（一般層）への普及は難しいであろう。

また、やはりこうしたサービスのネックは国ごとに異なる法律や規制への準拠である。2019年に米国FinCENが公表したガイドラインでは、秘密鍵を一切預からない形でP2Pの取引を補助するものは“ソフトウェア”として位置付けられ、秘密鍵を預かる形式のものは“ATM”に該当するとされている。米国では規制監督が一本化されておらず、これがすべてではないのだが、そうしたガイドラインもこのDeFiマーケットの追い風になったことは否めない。大きな事件が起きずこのまま発展し続けられるのか、またこのマーケットがアジアでどのように展開されるのか、どのような国や地域でこうしたサービスが普及していくのか、注目して見守る必要があるだろう。

■Proof of Stakeおよびステーキングの台頭

ブロックチェーンでもう1つ注目しているのがPoSとステーキングである。PoSはProof of Stakeの略で、ブロックチェーンの意思決定の根幹をなすコンセンサス参加方法のメカニズムである。パブリックブロックチェーンでの合意形成の際に悪意のある第三者による恣意的な合意をどのように防ぐかという観点で仕組みが作られている。

ご承知の方も多いと思うが、ビットコインはProof of Work（PoW）という仕組みで演算による作業量の証明を行っている。このため電気代が安価な国や地域にマイニングファームと呼ばれる大型の専門設備を設けることでマイニングを行っていた。しかしこれには巨額の先行投資が必要であり、消費電力も多い。2017年には世界中でのマイニングでの電力消費量がアイルランドの年間電力消費量を超えてしまうなど、効率の悪さと環境への問題が指摘されてきた。

そうした問題の解決につながるのではないかと注目が集まっているのがProof of Stakeである。PoSはバリデーターと呼ばれるマイニングにおけるノードを運用するアカウントをクラウドサービス上や各人のラップトップ上で構築・運用できるようになっているものである。バリデーターになるためには各ブロックチェーンのルールに則る必要があるが、その際ランダムにブロック生成タイミングが回ってくる。その確率も当該ブロックチェーンのネイティブトークンの保有量で変化するモデルなどが存在する。またバリデーターとしてブロックの生成が任命されたタイミングで生成や二重支払いの確認といった決められた動作を行うことで、ブロック報酬とネットワーク手数料が貰えるようになっている。このとき、たとえばラップトップの電源が落ちていたりインターネットにつながっていなかったり役目を果たせなかった際には、バリデーター本人のロックされたトークンの一部が自動的にブロックチェーンプロトコル自体に奪われるスラッシングと呼ばれる現象が起きる。マイニングで言えばマイニングマシンが突然燃えるようなイメージだが、これはマイニングにはありえないことである。あくまで保有トークン量を根拠にバリデーター権を得る。これがステーキングと呼ばれるもので、PoSならではのシステムである。

このPoSが普及し始めたきっかけは、PoSを採用した時価総額の大きなパブリックブロックチェーンが次々に登場したことが挙げられる。2019年にはInter-Blockchain Communication protocol (IBC)と呼ばれる他のブロックチェーンとの相互通信が可能になるシステムを取り入れたCosmosのほか、マサチューセッツ工科大のコンピューターサイエンスの教授でもあるシルビオ・ミカリ氏などの論文を元にしたAlgorand[3]のメインネット（パブリックブロックチェーン化）が公開されて話題を呼んだ。2020年はEthereum 共同設立者のギャビン・ウッド博士が中心となって開発を進めるフレームワークSubstrateを元にしたブロックチェーンPolkadotや、スケーリングに特化をしたSolanaなどのメインネットの公開が予定されている。PoSはそれぞれが異なるトークンを持つパブリックブロックチェーンであるため、こうしたPoSネットワークの林立は、ネットワークの相互運用性（インターオペラビリティー）の向上意識を高めることにつながるだろう。PoSで重要なことはトークンが存在するからこそトークンを用いてルールを変更できるといったガバナンスの要素である。前述のPolkadotではForklessブロックチェーンを謳っており、ハードフォーク（ブロックチェーンの分岐によりトークンがAとA´に増幅すること）なしでブロックチェーンプロトコルそのものをアップグレードできる仕様になっている。その際にネットワーク参加者の同意を確認するといった方法が必要となるが、パブリックブロックチェーン上で動作するトークンが存在していることで、それらトークンを元にユーザーの投票数などを設定でき、オンチェーンガバナンスと呼ばれる合意形成を投票によって実現している。しかしPoSの世界ではトークン所有者の1/3程度が悪意を持つ第三者に乗っ取られることで一定程度ネットワークに不正をもたらすことができてしまうことから、そうした悪意のある攻撃を防ぐトークンアロケーション（割り当て）が重要になるだろう。

■2020年に向けた課題

最後に2020年のブロックチェーン業界の課題をまとめておきたい。筆者が注目していることの1つはレイヤー2を用いた“ブロックチェーンの存在を意識せずに利用可能なアプリケーション”の普及である。もともとレイヤー2はスケーリングソリューションとして開発され、ビットコインなどの上でネイティブトークン（BTCやETH）をロックする形で高速処理が実行できる。ビットコインではLightning Networkが主要なものであり、これは直近ではBOLT(Basis of Lightning Technology)という共通規格が定められている。Lightning Networkは主にマイクロペイメントなどで活用が期待されている。ビットコインをレイヤー2で即時に送り合えるUXは、より多くの人たちが直感的にビットコインをストレスなく送信できるようになる未来を指し示している。実社会の課題解決につながるプロダクトがパブリックブロックチェーンという透明化ツールやスマートコントラクトを用いた人的オペレーションを省く自動化技術を用いて実装されるのはいつか、注意深く見守りたい。

1. 「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律」が2019年5月31日に公布、資金決済法・金融商品取引法が改正された。また、カストディ事業者とは同法に定める他人のために暗号資産の管理する事業者をいい、金融庁の事務ガイドラインに記載がある。
2. https://defipulse.com/　2019年12月30日調査
3. https://www.axion.zone/algorand-made-by-mit-cs-and-game-thery-team/

インターネット白書 ARCHIVES

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～2020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が、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