暗号資産サービスの概観と展望

坂井 豊貴｜慶應義塾大学経済学部 教授

要約

謎の人物サトシ・ナカモトが 2009 年にビットコインを公開して以来、さまざまなタイプの暗号資産と、暗号資産を軸とするサービスが世に登場した。それらサービスの特徴は、ユーザーに何らかの形で分散管理されていることや、売買や賃借といった経済行為が組み込まれていることだ。2022 年には「web3」というフレーズが人口に膾炙したが、これはそうした新型サービスのひとつの潮流を表すものだ。本稿ではそれらサービスを概観し、現状について筆者の見解を述べる。

坂井 豊貴

慶應義塾大学経済学部教授
ロチェスター大学経済学博士課程修了（Ph.D.）。2014 年より現職。Economics Design Inc. 取締役、プルデンシャル生命保険 社外取締役などを併任。
Astar Network、Gaudiy Inc、ONGAESHI プロジェクト等のクリプト事業に、アドバイザーとして従事。

1．ビットコインから無数の実験へ

2008 年 10 月 31 日に “Bitcoin: A Peer-to-Peer Electronic Cash System” という 9 ページの論文が暗号学のメーリングリストに投稿された。それはビットコインの設計を概観する、端正に書かれた学術論文だった（Nakamoto 2008）。投稿したのはサトシ・ナカモト。いまも正体不明の人物である。

2009 年 1 月 3 日にサトシはビットコインのシステムを稼働させた。そして数日後、誰でもビットコインに関われるよう世にネットワークを公開した。ビットコインはブロックチェーンという記録の技術を基盤としている。中央集権的に管理されたひとつの台帳ではなく、自律分散的に管理された複数の台帳たちがネットワーク全体で記録を管理するのがその特徴だ。一部の台帳が活動を停止したり改竄されたりしても、残りの台帳たちがネットワーク全体に正しい情報を伝播させるので、記録付けが堅牢である。

ビットコインのようにパブリック・ブロックチェーンと呼ばれるものは、誰でもその台帳の役割を担える。ビットコインについては自主団体 bitcoin.org のウェブサイトで、ビットコイン・コアというソフトウェアをダウンロードすればそれが出来る。世界の何処の誰が何人ほど台帳の役割を担っているかは不明であり、これはネットワーク全体を破壊するのがきわめて困難であることを意味する。

ビットコインの公開はビッグバンのような出来事であった。その後はブロックチェーン技術に基づくさまざまな暗号資産と、暗号資産を用いるサービスが誕生した。本稿ではそれらを概観し、筆者の見解を述べる。暗号資産は大別すると、いわゆる仮想通貨のようなものと、NFT と呼ばれる保証書のようなものがあるが、本稿では紙幅の制約上、前者に焦点を絞る。また、暗号資産やそれに関するサービスを総称して「クリプト」と呼ぶ。クリプトの急速な進化を可能としたのは無数の実

験的プロジェクトであり、それらへの理解を助けることが本稿の目的である。

2．暗号資産の用途とナラティブ

2－1　通貨という用途

ビットコイン（BTC）それ自体に機能はない。それは通貨として、つまり「交換の媒介」や「価値の保存」の手段として、サイバー空間で用いられるためのものだ。暗号資産としては最も単純と言ってよい。BTC 登場後には、送金速度やプライバシー保護機能などを改善した通貨として、ライバル的な暗号資産が多く現れた。初期のものには 2010 年に開発されたライトコイン（LTC）があり BTC より送金スピードが速い。LTC は今も比較的高い時価総額を維持しているが、これは例外的である。通貨としての用途しかもたない暗号資産は、一時期は高値になっても、すぐに失速して忘れ去られるのが常である。

ユーザー数が多いほど利便性が上がるというネットワーク効果が、通貨の価値の形成には重要である。そして、明日も明後日も人々が価値を認めるという予想が人々のあいだで成立していないと、誰も今日その貨幣を入手しようとは思わない。BTC のように圧倒的な存在感をもつ暗号資産が人々の信任を集めている状態で、新規のライバルが対抗するのは難しい。

しかも BTC は、これが人類にとって価値あるものだから守ろう、改善していこうという開発者のコミュニティによって支えられてもいる。自律分散とは、管理が不要という意味ではなく、不特定多数の管理者で管理をするという意味である。不特定多数の管理者のコミュニティの質は、そのまま通貨やプロジェクトの質に直結する。BTC が最初の暗号資産であることや、サトシ・ナカモトが残したエピソードは、BTC に神話のようなナラティブを与えている。オープンソースである BTC のコードはコピーできても、BTC がまとうナラティブは得られない。

2－2　ガス代という用途

BTC に次ぐ時価総額をもつイーサ（ETH）は、2015 年に運用が始まったイーサリアムネットワークの機軸通貨である。ETH は、イーサリアムネットワーク上でオンライン店舗を作ったり、その店舗でものを売買するときに、ネットワークを動かす利用手数料（ガス代という）として必要である。例えば筆者が OpenSea というオンライン店舗でデジタルアートを買うときには、売り手に ETH で購入代金を支払うのみならず、ネットワークに対して ETH でガス代を支払う。

イーサリアムネットワークでガス代として使える暗号資産は ETH だけであり、他は一切使えない。つまりイーサリアムネットワークに利用価値があるなら、ETH にはガス代としての用途が発生する。こうした用途をもつ暗号資産の方が、通貨としての用途しかもたない暗号資産よりも、価値をもつことは分かりやすい。そしてその価値を投資家に感じてもらえるかは、プロジェクトのナラティブに大きく依存する。クリプトのプロジェクトは暗号資産を投資家に売って資金調達をすることが通常であり、その際にナラティブが重要であることは言うまでもない。

なお、イーサリアムは取引を自動実行するスマートコントラクトの土台となるチェーンだが、同様の機能をもつ多くの後続チェーンが存在する。それらチェーン

も、やはり自身が発行する暗号資産を基軸通貨にして、利用者にガス代を求めるのが通常である。

2－3　投票権

暗号資産の用途として比較的実現しやすいのは投票権である。プロジェクトの意思決定において、投票権として使えるという用途だ。かりにプロジェクトに収益性がなくとも、それが社会的に意義あるものであれば、そこでの意思決定に参加することに人は一定の価値を認めるだろう。であればその暗号資産をもつことには価値があり、それゆえ価格がつく。投票権のように、プロジェクトの自治に参加する機能をもつ暗号資産をガヴァナンス・トークンという。暗号資産のプロジェクトは、世界中の誰でも参加できて意思決定に関与できるという分散性を尊ぶのが基本姿勢であり、ガヴァナンス・トークンはその姿勢ときわめて親和性が高い。

では、意義あるプロジェクトの意思決定に参加できることは、ガヴァナンス・トークンに高い価格をもたらすのだろうか。これはプロジェクトによる。意義あるプロジェクトへの参加に人が価値を感じるにせよ、意思決定への参加は面倒で望まないかもしれないからだ。選挙権に価値があるにせよ、選挙に行くのは面倒くさいというのと同じだ。それでもプロジェクトのナラティブがよくできていれば、「自分は投票はしたくないが、したい人も多くいるだろう。値上がりが期待できそうだから、そのガヴァナンス・トークンを買っておこう」という投資家心理を誘発できる。

2－4　配当権

ガヴァナンス・トークンの所有者は、投票を通じて「ガヴァナンス・トークン所有者に収益の一部を分配せよ」と要求できることが多い。この場合、ガヴァナンス・トークンは投票権と配当権を併せ持つ、株式会社の株のような存在となる。投資家は、プロジェクトの将来の収益性を高いと予想するなら、現在ガヴァナンス・トークンを買おうとする。配当をほとんどあるいは全く得られないガヴァナンス・トークンは、投票権の用途しかなく、投資家を惹き付けるのは難しくなる。

2－5　オークション

ポルカドットは、イーサリアム共同創業者の一人であったギャビン・ウッド氏が創始した、複数のブロックチェーン・ネットワークを「ハブ」的なブロックチェーンに連結させるプロジェクトである。自分のネットワークをハブに連結するメリットは、セキュリティを高められること、他のブロックチェーンとスムーズな価値交換をしやすくなること等である（Wood 2016）。

ポルカドットにはドット（DOT）という機軸通貨がある。ブロックチェーンの運営体が、限られた連結権をオークション（Polkadot Parachain Slot Auction）で競り落とすときには、DOT で入札する。つまり DOT にはオークションでの競り落としという用途がある。オークションの競り落としに用いられた DOT は、誰かの手に渡るのではなく、2 年間ロックされる。ロックは市場での DOT 供給量を減らすので、DOT 価格を上げる効果をもつ。日本と縁が深いプロジェクトでは、渡辺創太氏が率いる Astar Network が 2021 年 11 ～ 12 月に行われた第 3 回目

のオークションで連結権を競り落とした。ポルカドットのオークションでは、ネットワークの運営者のみならず、ファンも協力して入札できる。つまりファンを含むコミュニティ全体で、ネットワークをハブに繋ぐためのオークションに参加できる。このような活動は、おそらくこれまでの人類社会には存在しなかったものだ。

3．コミュニティと分散自律組織

Astar Network に限らず、一定以上成功しているプロジェクトには、ファンとそのコミュニティがある。Astar Network でいうと、ファンは基軸通貨のアスター（ASTR）をもっているのが通常で、彼ら彼女らは渡辺創太氏や Astar Network を応援すると同時に、ASTR が値上がりする活動に貢献しようとする。いわゆる「web3」と呼ばれるクリプトのムーブメントの核にあるのは、コミュニティによる分散的な所有と意思決定である。そもそもビットコインからして、それを根底で支えるのは、ビットコインの仕組みや意義を尊ぶファンや開発者コミュニティである。クリプトの市況が悪くなると、ファンでない者は BTC を売って市場から退場するが、ファンはもち続けて価格の維持に貢献する。

コミュニティを結束させるのは、理念への共鳴やファン心理、および金銭的な利害の一致である。そのように結び付いたコミュニティが、プロジェクトの運営体またはそれに近い水準まで達しているものを分散自律組織（Decentralized Autonomous Organization、DAO）という。分散自律組織は企業のように定型的なフォームをもつわけではないが、概ねそのようなものである。

暗号資産が投票券の用途をもつプロジェクトでは、暗号資産の所有者がプロジェクトの大きな決定権を持つ。このときプロジェクト作りとコミュニティ作りは分かちがたく結び付いている。そしてこのことは、プロジェクトの運営体が、株式会社という形態と必ずしも相性がよくないことを意味する。コミュニティと株主の利益が常に一致するわけではなく、株主総会がコミュニティの意思決定を尊重するとは限らないからだ。

だから現在または将来において DAO を運営体としたいプロジェクトによっては、株式会社やそれに類する法人形態を避けようとするものがある。しかし現実社会で事業をするためには、何らかの法人格がないと契約に不便であり、参加する個人が無限責任を負うことにもなる。DAO に適した法人形態の例には、ケイマン諸島での Foundation Company がある。これは会社と信託のあいだのような法人形態で、株主のような所有者がいないオーナーレス法人である。この法人の定款に「ガヴァナンス・トークンで意思決定をする」のように記述すると、Foundation Company の運営者はその定款を守る義務が法的に生じる。ケイマン諸島というとタックス・ヘイブンとしてネガティブなイメージをもたれがちだが、ここは DAO を実現できる貴重な実験場でもあるのだ。

4．資金調達

プロジェクト初期に暗号資産を売って資金を得て、そのお金で、その暗号資産が使えるサービスを作る。これは先に遊園地のチケットを売っておいて、その資金で遊園地を造るようなものだ。ただしそのチケットは証券のように売買できるので、

投資の対象となる。だから投資マネーがチケット売買に舞い込む。チケット的なものを事実上の金融商品にできる、というのがクリプトの特徴である。

資金調達のため暗号資産を売る方法を大まかに分けると、運営主体が販売を公表して広く買手を公募するICO（initial coin offering）、特定の管理者がいる中央集権型取引所で買手を公募するIEO（initial exchange offering）、特定の管理者がいない分散型取引所で買手を公募するIDO（initial decentralized exchange offering）等がある。

日本では記事を書いたり投げ銭を与えられるALISというソーシャルメディアのサービスが2017年9月にICOを実施し、約4.3億円を集めた。ALISのケースは、日本ではほぼ初の本格的なICOである。しかしその後、金融庁が規制を進めて、日本ではICOは事実上できなくなった。「事実上」というのは、日本の証券会社を通すとICOも法的にはできはするからだ。ただ、それをするには審査を受ける時間と金銭のコストがかかるうえ、買手はその証券会社のアカウントをもっている人に限定されるので、暗号資産のユーザー層とは重なりが狭い。これでは迅速に世界から買手を集められるICOの魅力がほとんどない。日本の取引所で行うIEOにも同様の欠点があるが、買手が取引所でアカウントをもっている人になるので、証券会社でICOをやるよりは活発に売れやすい。日本のIEO第一号は、NFTの総合プラットフォーム「Palette」を展開するHashpalette社がコインチェック社で実施したもので、約9.31億円を調達した。

IDOとは、IEOのようなことを分散型取引所で行うものだ。ただしIEOと違ってIDOには、良くも悪くも取引所によるプロジェクトの審査が入らない。

5．分散金融（DeFi）

暗号資産をめぐるさまざまなプロジェクトのなかでも、とりわけ実験性が高いのは分散金融（Decentralized Finance、DeFi）だろう。2018年11月にリリースされたUniswapはその代表格だ。これは誰でも自分の暗号資産Aを別の暗号資産Bに交換できる分散型取引所（Decentralized Exchange、DEX）である。Uniswapでは、ある暗号資産を、そのときの為替レートに応じて、別の暗号資産に換えられる。例えば1ETHを2000 USDCに換えられる。これができるのは誰かが「ETHとUSDC」の通貨ペアを流動性供給（liquidity provision）しているからだ。

数値例で説明しよう。いま自分が、ETHをUSDCに換えたいと思っており、Uniswapを訪れたとする。そこには他の人々が流動性供給のため預けた「ETHとUSDCのペア」のプールがある。いまプールされている「ETHとUSDCのペア」でのETH量をX=9、USDC量をY=18000とすると、Y/X=18000/9=2000である。このとき為替レートは1 ETH=2000 USDCで定まる。ここで自分が1 ETHをプールに置くと、代わりに2000 USDCを受け取れる。プールの中には変化が起こり、ETH量は9+1=10、USDC量は18000-2000=16000となる。そして今後は為替レートが1 ETH=16000/10=1600 USDCとなる。これがDEXにおける価格の内的調整である。

すると誰もがこのプールに、1:1600 の比で、ETH と USDC のペアを預けられる。預けるメリットは、その DEX のガヴァナンス・トークンや、為替手数料の収入を得られることである。ここでペアとして（2 ETH, 3200 USDC）をプールに預けたとしよう。するとプール内では、ETH 量が 10+2=12、USDC 量が 16000+3200=19200 と変化するが、価格は 1 ETH=19200/12=1600 USDC のままである。つまり流動性供給は為替レートに影響を与えない。

それでは DEX 内の為替レートは DEX 外の為替レートと一致するかというと、裁定取引をする投資家が一致させてくれる。もしいま DEX 外市場で 1 ETH = 1500 USDC であれば、投資家は DEX 外市場にて 1500 USDC を 1 ETH に交換して、DEX でその 1 ETH を 1600 USDC に交換すれば、100 USDC の儲けを得られる。すると DEX 内では ETH の量が増えて USDC の量が減るので、為替レートが下がって 1 ETH が 1500 USDC に近づく。これが DEX における価格の外的調整である。単純だが実によく出来た仕組みだ。

分散金融の仕組みは DEX だけではない。例えば、ある暗号資産を担保に預けて別の暗号資産を借りるレンディングといった仕組みもある。分散金融のサービスの多くは、日本を含む多くの国で、何かしら（例えば銀行や証券会社）の業法に引っかかる。だから運営者は、業法に引っかからない国でオンライン上の DEX サービスを運営して、他国のユーザーが自己責任で勝手に使う、という形態をとるのが通常である。かりに日本のユーザーが分散金融のサービスを用いて大きな不利益を被っても、誰かがそれを回復してくれるわけではない。

6　実需あるサービスへ

「To earn」と呼ばれるジャンルのサービスがある。ゲームで好成績を達成すると暗号資産を得られる Play to earn のゲーム Axie Infinity や、歩くと暗号資産を得られる Move to earn の STEPN というサービスがよく知られている。これらのサービスでは、ガヴァナンス・トークンと、配布される暗号資産であるユーティリティ・トークンを区別するのが通常である。そのようなトークン設計をデュアルトークン・システムという。

例えば Axie Infinity では、ガヴァナンス・トークンは AXS（Axie Infinity Shards）で、ユーティリティ・トークンは SLP（Smooth Love Potion）である。AXS には投票権や配当権といった用途があるが、SLP はゲーム内で用いられる通貨というだけで、必ずしも魅力的な用途があるわけではない。同様に、STEPN には GMT（Green Metaverse Token）というガヴァナンス・トークンと、GST（Green Satoshi Token）というユーティリティ・トークンがある。

一般的に、デュアルトークン・システムでのガヴァナンス・トークンは発行上限が決まっていたり、総量の増え方に上限が設けられているが、ユーティリティ・トークンにはそのような上限がない。運営体としては、ガヴァナンス・トークンは価値の希薄化を防ぎたいが、ユーティリティ・トークンについては柔軟にユーザーに配布したいのだと考えられる。ここで問題は、数量に上限がないうえ用途も乏しいユーティリティ・トークンは価格を維持しにくいことである。つまり Play to

earn や Move to earn といった斬新なテーマで話題を呼び、一時期はユーティリティ・トークンに高い価格が付いたとしても、有望な用途がない限り、その価格は続かず暴落してしまうのだ。するとサービスがもつ「To earn」の魅力は下がることになり、ユーザーが離れる。結果として、配当権をもつガヴァナンス・トークンの魅力も下がる。

結局サービスは、サービス外からお金を流入させないと配当を支払い続けられず、ガヴァナンス・トークンは価格を維持できない。このとき運営体や、運営体に出資したヴェンチャーキャピタルは、ガヴァナンス・トークンの販売によって収益をあげられない。2022 年には、この当たり前の事実が、暗号資産の界隈でかなりの程度、共通認識となったように見える。今後はデュアルトークン・システムのような仕組みだけでは、ガヴァナンス・トークンをヴェンチャーキャピタルに売って資金調達をすることは難しいだろう。

7．おわりに

ビットコインが人口に膾炙し始めた時期には「いかに決済に便利な通貨であるか」が重要なナラティブであったが、最近では「いかにお客様に価値を提供してお金を払っていただくか」が重要になったと筆者は見る。そして価値を提供してお客様にお金を払っていただくとは、通常の商売が行っていることだ。それができるサービスの設計は、ブロックチェーン・エンジニアや金融出身者らだけでは難しく、元々実需あるサービスを運営している大手企業が有利である。これはフェイズの大きな変化だ。

実需あるサービスに暗号資産を絡ませた方が儲かるかは、サービス形態による。例えばこれからオンラインスクールを運営するとして、サービス開始前に受講料として使えるトークンを販売するか、トークンは発行せずサービス開始後に日本円で毎月受講料を払ってもらうか、どちらがより儲かるだろう。前者のほうが早い段階でキャッシュを得られるが、まだサービスが存在しない段階ではトークンに高い価格が付かないかもしれない。トークンに夢のようなナラティブを乗せて売ることが難しくなった、というのが現状であろう。2022 年 11 月には預かり金の使い込みや不正会計によって、取引高世界第 2 位の取引所 FTX トレーディングが経営破綻した。クリプトへの規制が米国をはじめ多くの国で強まるのは確実だ。これも小規模なチームやスタートアップ企業よりも、大手企業に有利な展開であろう。

引用文献

- あたらしい経済「ALIS の未来とこれからの ICO の可能性について / 安昌浩 CEO インタビュー（後編）」https://www.neweconomy.jp/features/alis/26269
- 天羽健介、増田雅史 編（2021）『NFT の教科書 ビジネス・ブロックチェーン・法律・会計まで デジタルデータが資産になる未来』朝日新聞出版
- 亀井聡彦、鈴木雄大、赤澤直樹（2022）『Web3 と DAO 誰もが主役になれる「新しい経済」』かんき出版
- コインチェック株式会社「Palette Token の販売結果に関する開示情報」2021 年 https://

drive.google.com/file/d/1Ae60AlthISgfylRCzjhzrLk_14jWlfSU/view
- 坂井豊貴（2019）『暗号通貨 vs. 国家　――ビットコインは終わらない』SB 新書
- 増島雅和、堀天子 編著（2020）『暗号資産の法律』中央経済社
- Hayden Adams, Noah Zinsmeister, and Dan Robinson (2020) “Uniswap v2 Core” https://uniswap.org/whitepaper.pdf
- Axie Infinity Whitepaper, https://whitepaper.axieinfinity.com/
- Conyers Dill & Pearman (2021) “Cayman Islands Foundation Companies” https://conyers-cdn.scdn5.secure.raxcdn.com/wp-content/uploads/2021/02/Foundation_Companies-CAY.pdf
- Satoshi Nakamoto (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System”
- https://bitcoin.org/bitcoin.pdf
- STEPN Whitepaper, https://whitepaper.stepn.com/
- Gavin Wood (2016) “Polkadot: Vision for a heterogeneous multi-chain framework,” Draft 1, https://polkadot.network/PolkaDotPaper.pdf