伝統的金融に呑まれる分散型金融

― 暗号資産 ETFと合同会社型 DAOを例に考える ―

斉藤 賢爾｜早稲田大学大学院経営管理研究科教授

要約

2024 年 1 月から 5 月にかけて、米国にて BTC や ETH といった暗号資産の現物価格を指標とする ETF（Exchange Traded Funds）が承認されたり、我が国において合同会社型 DAO（Decentralized Autonomous Organization）が法的に認められたりといった規制緩和が行われ、一般公衆が暗号資産に基づく分散型金融（Decentralized Finance）にアクセスしやすくなったとして注目を浴びている。これらの新しい金融商品や組織形態は、伝統的金融と分散型金融の双方の歩み寄りの結果のようにも見えるが、伝統的金融との接点を必ず必要としていた暗号資産交換業と同じ問題を抱えることになるのではないだろうか。本稿では、暗号資産とブロックチェーンのそもそもの成り立ちを振り返りながら、これらの新しく見える概念について、その意味を改めて議論する。そのことを通して、最初から伝統的金融なくしては成り立たず、伝統的金融に呑まれていた分散型金融の姿が見えてくる。

斉藤 賢爾

早稲田大学大学院経営管理研究科教授

コーネル大学より計算機科学において工学修士号、慶應義塾大学よりデジタル通貨の研究で博士号を取得。日立ソフトウェアエンジニアリング、慶應義塾大学大学院政策・メディア研究科特任講師等を経て現職。

1．はじめに

2024 年 1 月と 5 月、米国では証券取引委員会（SEC）が Bitcoin（Nakamoto, 2008）のネイティブ暗号資産[1]である BTC と Ethereum（Buterin, 2013）のネイティブ暗号資産である ETH の現物価格を指標とする ETF（Exchange Traded Funds; 上場投資信託）を相次いで承認した[2]。一方、同年 4 月、我が国では金融商品取引法に関わる内閣府令の改正により、法人格を持てる合同会社型 DAO（Decentralized Autonomous Organization; 分散型自律組織）が可能となった。

これらによって、一般の消費者が適切な保護や法的な裏付けの下で暗号資産に基づく分散型金融（Decentralized Finance）や分散型自律組織にアクセスできるようになると見込まれることから、こうした最近の動きは多くの人々により好意的に迎えられているように見える。この現象は、伝統的金融が分散型金融に歩み寄ったということなのだろうか、それとも分散型金融が伝統的金融に呑み込まれたのだろうか、あるいはその両面があるのだろうか。

1：本稿では、ブロックチェーンの維持活動に参加することで新規発行分を得られる暗号資産を、そのブロックチェーンのネイティブ暗号資産と呼ぶ。各ブロックチェーンではそうではないデジタル資産を定義し、その所有権の移転を記録することもできる。

2：ETH の現物 ETF に関しては、2 段階の承認プロセスの最初の段階が 2024 年 5 月に承認されたのであって、最終的な上場承認はこの稿の執筆時点では未だ成されていなかったが、同年 7 月に承認された。

本稿では、暗号資産とブロックチェーンのそもそもの成り立ちから振り返ることを通して、暗号資産の現物価格を指標とする ETF や合同会社型 DAO といった新しく見える概念について、その意味を改めて議論する。これらの金融商品や組織形態は、伝統的金融と分散型金融の双方の歩み寄りの結果のように見えるかも知れないが、その背景には、元々伝統的金融なくしては成り立たないという、分散型金融の根幹が見落とされていると筆者は考える。本稿は、最終的に「分散」と「集中」の対立軸に焦点を当て、分散型金融が本来持つ意味とその実状を露わにする。

2. 暗号資産の成り立ちを振り返る

2.1 設計のゴール

サトシ・ナカモトを名乗る人物ないし集団が、最初のブロックチェーンであり暗号資産システムである Bitcoin について初めて記述した設計文書（Nakamoto, 2008）は、その冒頭で、信用できる第三者としての金融機関を通した送金[3] を問題視していた。そのような第三者は原理的に送金を検閲でき、口座の凍結といった形で資金の移動を否定できるからである。したがって、Bitcoin の設計のゴールは、そのような第三者を排した、何人によっても検閲できない送金システムであり、「自分が持つ資金を自分が選んだ誰かに自由に送るのを誰にも止めさせない」ことの実現だと考えられる。

この要求は、次の 4 つの性質に分解できる。

1. 自己主権性 —利用者自身の意思のみによって利用者はシステムに参加でき[4]、送金を指示できる。

2. 狭義の耐検閲性 —利用者が指示する送金は、他の誰の意思によっても止められない。

3. 耐障害性 —利用者が指示する送金は、システムの故障・障害によっても止められない。

4. 耐改ざん性 —送金の記録は後から削除・変更できないし、過去に無かった送金の記録も捏造できない。

これらすべてを満たすことで、広義の耐検閲性（何人・何事によっても記録を否定できない）が実現される。

2.2 設計の概要

どのような技術であれ、無条件にその力を発揮できるわけではなく、例えば腕時計には、正常に動作する温度範囲が（あくまで例として）-10 ～ 60℃といった仕様がある。ブロックチェーンも同様に、特定の条件下で上の 4 つの

3：オンラインシステムでは支払いも送金によって実現されるので、支払いと送金は区別されない。

4：誰の許可も得ずとも自らの意思だけでアカウントを作れることを意味し、典型的には公開鍵と秘密鍵の鍵ペアを自分（のウォレット）で生成し、公開鍵をアドレスに変換し、秘密鍵を用いた演算（デジタル署名）によりそのアドレスが示す本人であることの認証を行う。

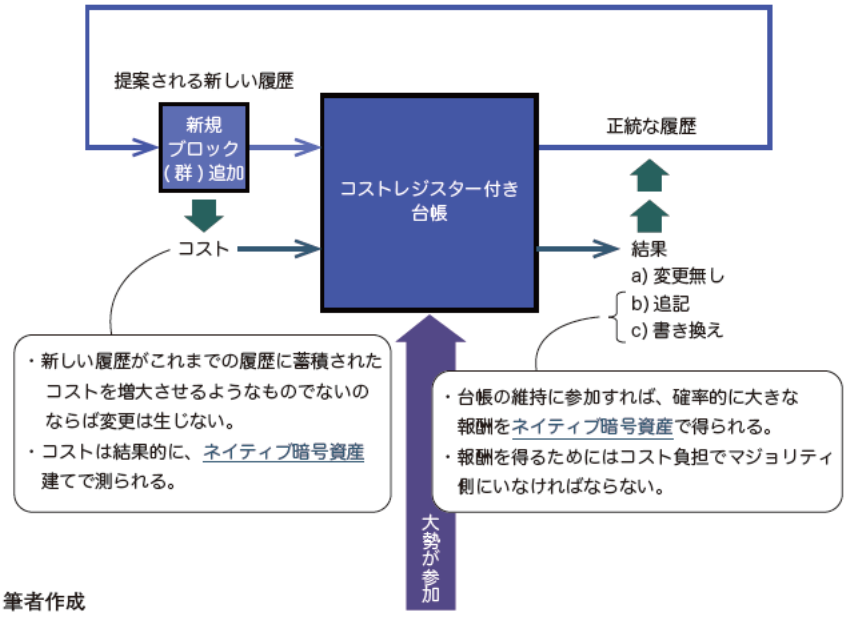
性質を満たすように設計された技術であって、条件から外れた状況では広義の耐検閲性が満たされるとは期待できない。では、ブロックチェーンの動作条件とは何だろうか。

そのことに留意しながらブロックチェーンの仕組みを説明するために、筆者が（Saito and Yamada, 2016）にて導入した、「コストレジスター付き台帳」というメタファーを用いることにしたい（図 1）。これは、台帳（ブロックチェーン）への記録が行われる際に投入されたコストをレジスター（登録器）に加算していき、蓄積されたコストが現状よりも大きくなる、すなわち記帳には追加コストが必要であり、それを誰かが実際に負担した場合のみ新たな記録を許す仕組みで、正統な送金履歴を維持する回路のようなものである。この台帳ないし回路は、大勢がその維持のために参加するインセンティブ構造を持つ仕組みとなっている。

利用者たちによる送金の記録はそうした大勢によって集められ、ブロックと呼ばれる構造にまとめられ、台帳に書き込まれる。ブロックは大勢のうちのひとりだけが作成し提案できる。送金履歴はブロックの列として表現されるが、これがブロックチェーンという名前の由来である。

新たなブロックが提案され追加される際には、それを認める大勢により大きなコストが負担される。 Bitcoin に代表される Proof of Work 方式の場合、そのコストはブロックの提案者を選ぶくじ引きのために各々が負担する電力コストであるが、後述するように各参加者は報酬による収益を期待してそのコストを負担するため、その上限はネイティブ暗号資産建て報酬の市場価格の期待値となる。 Ethereum に代表される Proof of Stake 方式の場合、そのコストは各々がネイティブ暗号資産建てで負担するデポジットおよび各自が正統と見なす履歴に対する投票であり、正統な履歴はデポジット換算で全体の$\frac{2}{3}$以上の票を集め続ける必要がある。

図1　暗号資産の成り立ち



出所）　筆者作成

コストレジスター付き台帳は、ブロックが追加された新しい履歴とそれに伴うコストを入力として受け取り、結果（変更無しか、履歴に追記するか、あるいは履歴を書き換えるか）と新たな正統な履歴を出力する。新しい履歴のコストが、現在の正統な履歴のコストを上回らなければ（すなわち、履歴更新にかかるコストが正でなければ）、変更は生じない。変更は、典型的にはひとつのブロックの追記だが、ある特定の過去から最新までの一連のブロックが改めて提案し直され、それによって履歴が置き換わる（reorg、すなわちチェーンの再構成と呼ばれる）場合もありうる。

満たすべき ４つの性質のうち、「自己主権性」はアドレスの設計により担保され、「狭義の耐検閲性」と「耐障害性」は、大勢が独立した運用方針をもって各々のコンピューターを参加させ、その結果、誰かが止めたい取引でも他の誰かによって記録が行われたり、誰かのコンピューターが止まっていても他のコンピューターが動いていたりといった冗長性がもたらされることによって担保される。そして「耐改ざん性」は、改ざんしようとする主体が単独では履歴の書き換えのためのコストを負担できないことにより担保されるため、コスト負担ベースで悪意はマイノリティなことが前提となる（下線部がブロックチェーンの技術的な動作条件であり、これらが成立するための動機的な条件を後述する ）。

台帳の維持に参加すると、確率的に大きな報酬を、そのために無から生み出されたネイティブ暗号資産で得られる。報酬を得るためにはコスト負担でマジョリティ側にいる必要があるが、このことでマジョリティが形成されやすくなり、履歴がまとまりやすくなる。

以上では台帳には送金が記録される前提で説明したが、台帳にはプログラムコードやその呼び出し、その実行結果を記録することもできる。それがスマートコントラクトである。スマートコントラクトを金融に応用したものが分散型金融だと言える[5]が、本稿では加えてネイティブ暗号資産の取り扱いも分散型金融の概念に含めている。

5：ブロックチェーンの ４つの性質を満たさない、プライベートな台帳上でのコード実行も含めて分散型金融だと主張する向きもあるため、この定義は狭いものだと言える。

2.3 暗号資産と DAO

Ethereum の共同作者のひとりであるヴィタリック・ブテリンは、ブログ記事（Buterin, 2014）にて DAO をこう定義した。「インターネット上に自律的に存在するが、自動システム自身にはできない特定のタスクを担うために人間を雇うことに大きく依存しており、そのために内部に資本（報酬として使われ人間を駆動する）を持つ。」

これは、ある意味ブロックチェーンのイメージそのものであり、ブロックチェーンこそが DAO の原型であるとすら言える。ブロックチェーンは、無からネイティブ暗号資産を生み出し、それを資本として参加者である大勢の人間を金銭インセンティブを通して雇い、駆動し、かつネイティブ暗号資産建てで計量されるコストによって台帳を改ざんから守っているからである。

このことが成立するためには、ネイティブ暗号資産が市場で十分に高値を付けている必要がある。安ければ大勢の人間を駆動できないし、ブロックチェーンを改ざんするためのハードルが低くなるからである。ブロックチェーンが正

常に動作するための動機的な条件は「ネイティブ暗号資産の市場価格が十分に高いこと」なのである。

2.4 価格形成

それでは、ネイティブ暗号資産の市場価格はどのように形成されるのだろうか。商品の価格は、一般に需要と供給のバランスによって決まる。需要が高まれば価格が上昇し供給が増えて需要とマッチし、需要が低まれば価格が下降し供給が減ってやはり需要とマッチする。需要の変化に対しては、一般に供給が反応することで価格の大きな変動は抑えられる。

一方、ネイティブ暗号資産に関しては、こうした供給の調整が成り立たないことを筆者らは Iwamura et al.（2019）および Saito and Iwamura（2019）にて議論した。ネイティブ暗号資産の新規供給はブロック提案の報酬として行われ、ブロックは一定の時間間隔で提案される設計であるため、需要の変化に対して供給は反応しない。したがって、需要が高まるほど価格は上昇し、需要が低まるほど価格は下降してしまう。

加えて、Bitcoin では 21 万ブロック毎に報酬が半減するいわゆる半減期を通して新規供給を減らし、最終的には全体の供給量が固定になることを目指している。また、筆者らが Saito et al.（2023）にて議論したように、Ethereum には半減期は無く、参加者数に応じて一定の割合で ETH が新規供給されるが、トランザクション（取引）の実行の基本手数料として支払われる ETH がバーン（消滅）されることを通して全体の供給量を一定に保とうとしている。需要が高まり、多くのトランザクションが発生すると、逆に全体の供給量は減ることになる。

さらに問題になりうるのは、暗号資産は産業と無関係に売買される点である。といっても、Bitcoin に代表される Proof of Work 方式の場合、くじ引きの計算の効率化に向けて半導体事業への投資を促し、また、より効率的な発電方法や、批判を避けるべく環境負荷の低い発電方法への移行を促すとも言える。対して Ethereum に代表される Proof of Stake 方式はネイティブ暗号資産によるデポジットによってシステムを保護する考え方であり、産業との接点を持たない。スマートコントラクトも主として分散型金融分野のアプリケーションであり、その多くも同様に産業との接点を持たないとすれば、単に需要を高めれば手持ち資産の価格が上がり、需要を低めれば手持ち資産の価格が下がる装置として利用されるに過ぎないことになってしまう。

3. 伝統的社会からの歩み寄り

3.1 前提となる接点

ブロックチェーンが正常に動作するための動機的な条件は「ネイティブ暗号資産の市場価格が十分に高いこと」なのだから、ネイティブ暗号資産の取引市場が存在する必要がある[6]。

そのため、多くの暗号資産交換業者が国内外で事業を行うニーズがあるわけ

6：2009 年に Bitcoin が稼働を始めた時点ではそのような市場は無かったが、技術的な興味によってブロックチェーンが維持されていたと考えられる。

だが、多くはドルや円といった旧来の通貨で暗号資産の売買が行われており、暗号資産の価値評価において、米ドルといった伝統的金融における通貨建ての価値が参照されている。この意味で、暗号資産の取引市場は分散型金融と伝統的金融との接点だと言える。

こうした多くの事業では、取引所・販売所の顧客間や交換業者との間で暗号資産の残高を付け替えることで取引が実行され、顧客が明示的に自分のウォレットへの引き出しを指示するまで、実際にはブロックチェーンには暗号資産の所有の移転は書き込まれない（ブロックチェーン上の取引手数料を節約し、かつ高速に売買を成立させるため）。ということは、こうした市場で売買されているのは、暗号資産の現物により裏付けられた何か、すなわち、交換業者によって管理される、ブロックチェーンとは別物の台帳の上に記録された暗号資産の所有残高である。そう考えると、すでに現物 ETF に相当するような抽象化が日常的に行われていたとも言える。

また、ブロックチェーン自体をその原型としていたと考えられる DAO も、「自動システムによって人間が雇われる」という部分が「雇われて業務を執行している社員たち自身により組織が所有されている」といったように解釈が緩和・拡張され、スマートコントラクトによる経営ルールと、同じくスマートコントラクトにより生成されたガバナンストークン[7] の持ち分に応じた投票権により組織の意思決定を行うタイプの DAO が乱立するに至った。これは基本的にはトークンの二次市場での値上がりを期待する勢力が参加者の大部分を占め、暗号資産の取引市場と同じマインドセットにより DAO が支配されてしまう類のものである。こうした現象は、元々の DAO の概念が伝統的社会における既存の株式会社や合同会社の概念に引っ張られて変化したものだと考えられる。

こうした動きを支えているのが、いわゆる「クリプト界隈」と呼ばれる、暗号資産の利用者の集合でありコミュニティである。クリプト界隈と一般の投資家たちの間には、リスクの捉え方にギャップがあり、暗号資産自体のボラティリティの大きさもさることながら、取引所・販売所のセキュリティーのリスク（サイバー攻撃や、詐欺や価格操作など）への寛容度の違いが、一般投資家の参加へのハードルとなっている。

7：トークンは代替貨幣の意味で、ここではスマートコントラクトにより生成されたデジタル資産を表す。

3.2 暗号資産の現物価格を指標とする ETF

2024 年 1 月 10 日、米国証券取引委員会（SEC）は BTC の現物 ETF を承認した（SEC, 2024a）。ETF の発行者は暗号資産取引市場から BTC を購入し、カストディ（管理・保管）サービスを通して保全し、ETF の裏付け資産とする。市場での BTC の購入と売却を通して、BTC 現物 ETF の放出と回収は BTC の市場価格に影響を及ぼしうる。

SEC は、同様の ETF の提案を、詐欺や価格操作のリスクを理由に長らく不承認としてきた。しかし、コロンビア特別区（ワシントン D.C.）巡回控訴裁判所が、そうした提案のひとつである Grayscale Bitcoin Trust（GBTC）に対する SEC の決定を無効とする判決を 2023 年 8 月 29 日に下したため、再検討を余儀なくされた（Gensler, 2024）。その再検討において、SEC は、

CME（Chicago Mercantile Exchange）の BTC 先物市場といった、現物市場と十分に相関関係が見られる取引所との監視共有契約がある場合は、提案された BTC の現物 ETF に関連する潜在的な詐欺や操作を監視する適切な手段が確保されていると判断した。これらの提案が市場の透明性、公平性、および効率性を促進すると同時に、投資家を詐欺や価格操作のリスクから保護することができるという信念のもと、承認の決定が行われたわけである。

同年 5 月 23 日、SEC は ETH の現物を裏付け資産とする ETF を承認した（SEC, 2024b）（上場に至る承認プロセスの第 1 段階）。

この場合においても、CME の ETH 先物市場と現物市場間の相関に基づく詳細な相関分析が提供され、SEC は、ETH の現物 ETF 市場での不正や操作が CME の ETH 先物価格に同様の影響を与える可能性が高いと結論付け、その結果、CME との包括的な監視共有契約が、提案された ETH 現物 ETF に影響を及ぼす不正や操作を監視する上で有効に機能すると期待したのである。

このように、暗号資産の現物 ETF は、暗号資産の現物に裏付けられた何かを売買するという暗号資産取引市場の考え方をある意味踏襲したまま、それをさらに一般の投資家が参加する伝統的金融の世界に引き込むべく、安全性に関わる手当てをしたものだと言える。

3.3 合同会社型 DAO

LLC（Limited Liability Company; 有限責任会社または合同会社）を DAO 化し、既存の法体系にあまり手を加えずに DAO を法人化する考え方は、米国ワイオミング州（Wyoming, 2022）をはじめとして各地で見られる。ワイオミング州の法律では、既存の LLC を DAO に転換することもでき、LLC が DAO と互換性があると考えられていることを示している。

我が国においても、2024 年 4 月 22 日に施行された「金融商品取引法第二条に規定する定義に関する内閣府令の一部を改正する内閣府令」および改正された「金融商品取引法等に関する留意事項について（金融商品取引法等ガイドライン）」（金融庁，2024）に拠り、合同会社型 DAO の設立が可能となった。

合同会社は、所有と経営が分離されていない会社（持分会社）の形態のひとつであり、出資者（社員）が経営を行い、原則として全員一致で定款変更などを行い、社員自らが会社の業務を執行する。合同会社型 DAO は、既存の合同会社の枠組みにブロックチェーン技術を組み合わせ、社員権を表すトークンやその他のトークン（別トークン）を発行することで資金調達ができ、また、トークンを保有する社員やその他の参加者による、例えば投票を用いたガバナンスを可能としている。

一般に DAO はガバナンストークンの買い占めによるテイクオーバー（買収）が可能であるが、合同会社型 DAO では業務執行社員権トークンの譲渡は相手も業務執行社員である場合にのみ可能であるので、合同会社と同様（というよりも法的にも合同会社であるので）、歓迎しない買収のリスクを避けられる。また、社員全員が自分の出資分だけの責任を負う有限責任を持つし、中でも債務者から直接弁済の追及を受けない間接有限責任を負うことで守られる。

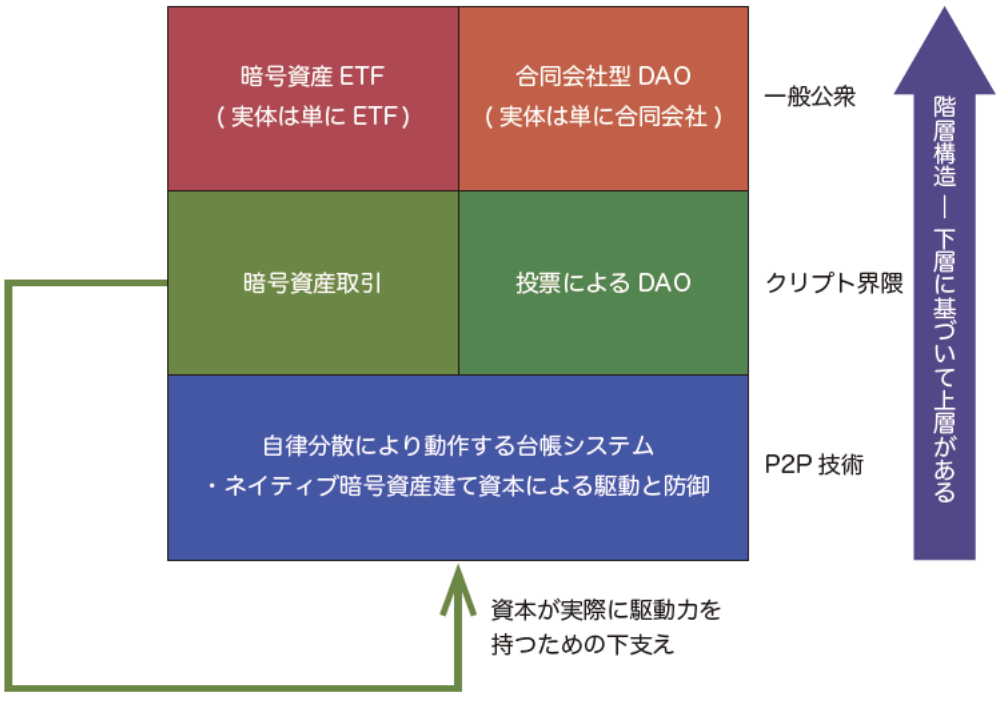
このように、合同会社型 DAO は、ブロックチェーンのインセンティブの構造として登場した原型としての DAO を株式会社・合同会社寄りに拡大解釈した「投票による DAO」を、さらに既存の合同会社として法的に解釈可能にし、法による保護を手当てしたものだと言える。

4. 分散型金融は伝統的金融に呑まれるのか

4.1 最初から呑まれていた分散型金融

さて、以上のように、暗号資産の現物 ETF や合同会社型 DAO といった新しい概念は、一般の消費者・投資家に対して十分な保護を提供することで、暗号資産へのアクセスを容易かつ安全にした。このことの背景には、図 2 に示すような階層構造がある。階層は、下層に基づいて上層があることを示す。

図2　暗号資産と DAOの階層構造



出所）　筆者作成

P2P（Peer-to-Peer）技術、すなわちネットワークに参加するコンピューターが対等に役割を担い、故障や妨害に強い柔軟なサービスを構築できる仕組みの賜として、ブロックチェーンという、自律分散により動作する台帳システムが作られた。そして、ブロックチェーンの上でネイティブ暗号資産が作られたり、スマートコントラクトを実行できることが前提となって、暗号資産取引や投票による DAO が可能となった。また、暗号資産取引市場が存在することが前提となってその ETF 化が可能となったし、投票による DAO が合同会社との類似性をもつことから合同会社型 DAO、すなわち社員権のトークン化が可能となった。これらの実体はそれぞれ単に伝統的社会における ETF であ

るし、合同会社（の社員権）である。

ここで忘れてはならないのは、ブロックチェーンはネイティブ暗号資産建て資本によって人間を雇い、駆動し、またネイティブ暗号資産建てで計量できるコストの高さによって守られているのだから、暗号資産取引市場（によってネイティブ暗号資産に高値が付けられること）に依存しているということである。

先に述べたように、暗号資産取引は伝統的金融との接点であり、ネイティブ暗号資産に付けられる高値は伝統的金融の価値で測られるのであるから、分散型金融は伝統的金融に最初からすでに呑まれていたのである。

4.2 考えうるリスク

原理が異なるものに呑み込まれているのだから、分散型金融の挙動は、ブロックチェーンが正常に動作するための条件から外れる恐れがあるし、伝統的金融の期待にも応えられない局面が生じうる。

その例としてリスク分散がある。ブロックチェーンのネイティブ暗号資産は需要が高まれば価格が上がり、低まれば価格が下がるのだから、単に別種の金融商品に投資をする選択肢として暗号資産を選ぶだけではリスクが分散されるとは限らない。例えば、株式市場と暗号資産取引市場の値動きに負の相関があるという期待があるとする。株の値段が下がるときに、株を売って暗号資産を買うという行動が需要の趨勢を決定づけるのであれば、実際にその局面で暗号資産の価格が上がる。これは予言の自己成就のメカニズムであり、最初に予言があり、その予言が市場の参加者に周知されていることが必要なのである。

SBI 金融経済研究所が行ったアンケート調査の結果（SBI 金融経済研究所, 2022, 2024）では、暗号資産に関する認識を問う設問に「投資対象を値動きの異なる金融商品に分散することで、投資のリスクを低減する効果がある」という選択肢があり、暗号資産への投資に関するリスク分散の可能性についての認知が一部の回答者にはあるものの、全体的な浸透度は必ずしも高くはないことが示された。このことは、仮に今後、暗号資産の現物 ETF が広く投資家の関心を集めたとして、人々が思うほどにはリスク分散の効果が出ない可能性にも留意すべきことを示唆しているのかも知れない。

また、現物 ETF の承認が各ブロックチェーンのネイティブ暗号資産価格の上昇に寄与するという期待は理解できるが、逆に将来的にそうした暗号資産の価格が暴落する可能性も無視できない。以下はそのようなシナリオを引き起こす可能性のある要因である。

- 市場の過熱：ETF の承認が大きな期待を生み、短期間で暗号資産の価格が急騰する可能性がある。しかし、このような急騰はしばしば市場の過熱を示唆し、商品貨幣のように本源的価値が存在せず、発行体に対する請求権がある負債性資産でもない暗号資産に市場価格が付くこと自体がバブルであり、過去の暗号資産価格の暴騰暴落を見ても、投機的バブルの発生の可能性は高い。期待が現実に見合わない場合、その後の価格調整は急激な暴落を引き起こす可能性がある。

- 流動性の問題：ETF への投資が増えると、その裏付けとなる資産への需要も増加する。しかし、ある時点で、市場における売り手が買い手を上回り、ETF 市場とその対象資産市場（暗号資産市場）の両方において流動性の問題が生じる可能性がある。これは価格が急落する要因となりうる。
- 規制リスク：金融商品としての ETF の承認により、暗号資産への規制当局の注目が高まる可能性がある。将来的に、より厳しい規制が導入されると、市場の不確実性が増し、投資家の信頼が損なわれ、結果として価格が下落する可能性がある。
- 技術的な課題：将来の暗号技術や量子アルゴリズムの飛躍的な進歩や、現時点で未知の脆弱性を突いたサイバー攻撃等により、ブロックチェーンのセキュリティーに関する未解決の問題が露呈する可能性がある。これらの技術的な問題が表面化すると、投資家の信頼が揺らぎ、価格が下落する可能性がある。
- 市場心理：投資市場での心理的な要因は価格に大きな影響を及ぼす。一旦、市場センチメントが転換し、恐怖が支配すると、パニック売りが起こり、価格の急落を引き起こすことがある。
- マクロ経済要因：グローバル経済の状況、金利の変動、通貨の動向など、暗号資産市場の外の要因も価格に大きな影響を及ぼす。これらの要因が不利な方向に進むと、暗号資産全体の価格下落を引き起こす可能性がある。

ただし現状では、価格が下降すれば、将来の上昇を見込んで買う投資家が現れる。このことで、これまでは主要な暗号資産については存続が危ぶまれるほどの過度な暴落は避けられてきた経緯がある。

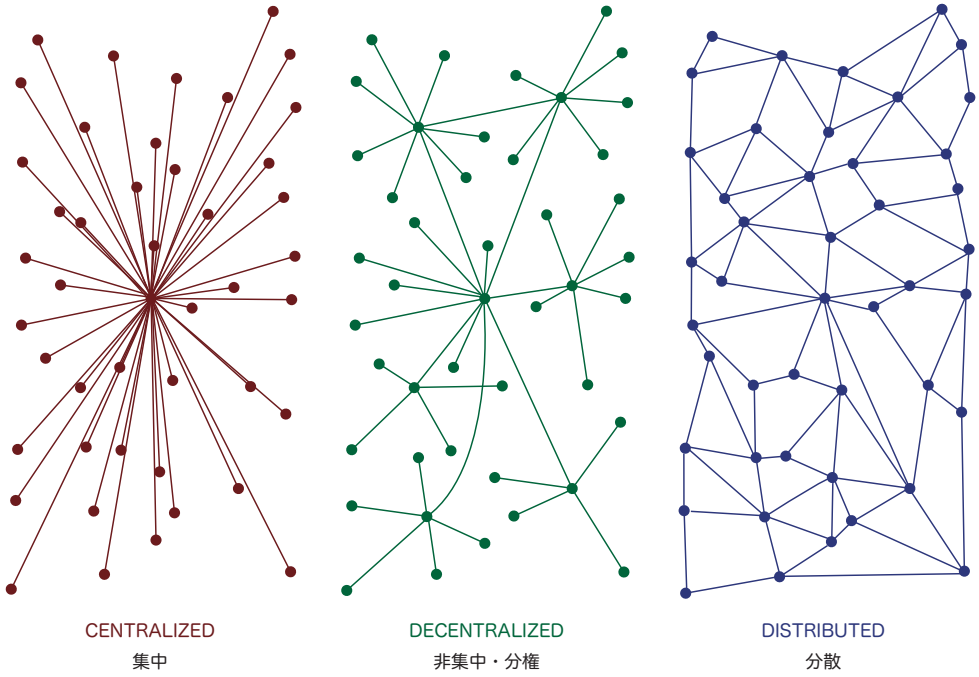
しかし、ブロックチェーンの原理に照らせば、ネイティブ暗号資産の市場価格の低下はそれ自体がリスクなのだから、実際にブロックチェーンの維持参加者の撤退が起きてもおかしくはない。暗号資産取引市場とブロックチェーンには、原理の乖離がある。

実際にブロックチェーンが維持できなくなった時、下層である基盤が揺らぐのだから、暗号資産の市場自体が崩壊すると考えられる。

おわりに

いわゆるクリプト界隈では、DAO や DApps（Decentralized Applications）といったように、“Decentralized”という言葉が好んで用いられる。これは、おそらくは“Centralized”（集中・中央集権）な伝統的金融に対するアンチテーゼとしての言葉の用い方で、Decentralized Finance に対する訳語「分散型金融」が示しているように、意図としては「分散」という概念を表したいのだろう。しかし、Baran（1964）に見られるように、コンピューターサイエンスの分野では、遅くとも 1960 年代から、“Decentralized”は多くの中心に権限が分かれる「非集中・分権」を表す言葉として明確に定義され、用いられてきた（図 3）。

図3　集中（centralized）、非集中･分権（decentralized）、分散（distributed）



出所）　Baran（1964）　Fig.1に基づいて筆者作成

P2P 技術の賜である台帳システムのネットワークは、特定の構造を持たずに実際に分散（distributed）（図 3 の右）なのだが、暗号資産取引や投票による DAO のネットワークは、期せずして様々な取引所・販売所やスマートコントラクトといった多数の中心を持つ構造であり、非集中・分権（decentralized）（図 3 の中央）である。それが悪いわけではないが、考えていることと実体の間に乖離がある。そしてこの構造は、多数の金融機関のネットワークが相互に接続された伝統的金融と同じ形なのである。

分散を志しながらも、伝統的金融との接点を通してしか自らを維持できない台帳システム自体に問題の根幹はあると言えるのかも知れない。何人・何事によっても記録を否定できないような台帳の存在自体は有益であるので、そろそろ、伝統的金融には依存しない、別の動作条件の下で動作する台帳システムに向けて、私たちの開発の労力を振り向ける時機が到来したと言えるのではあるまいか。

謝辞

この稿の執筆に当たり議論とインスピレーションをもたらした、早稲田大学大学院経営管理研究科「ブロックチェーンと分散ファイナンス」ゼミ（2024年度）の学生諸氏にこの場を借りてお礼を申し上げたい。

参考文献

Baran, P. (1964). On Distributed Communications: I. Introduction to Distributed Communica.tions Networks. RAND Corporation, Santa Monica, CA.

Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/.

———— (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

Gensler, G. (2024). Statement on the Approval of Spot Bitcoin Exchange-Traded Products. https://www.sec.gov/newsroom/speeches-statements/gensler-statement-spot-bitcoin-011023.

Iwamura, M., Kitamura, Y., Matsumoto, T., and Saito, K. (2019). Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money. Hitotsubashi Journal of Economics, 60(1).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf.

Saito, K. and Iwamura, M. (2019). How to make a digital currency on a blockchain stable. Future Generation Computer Systems, 100:58.69.

Saito, K., Soejima, Y., Sugiura, T., Kitamura, Y., and Iwamura, M. (2023). Is Ethereum Proof of Stake Sustainable? － Considering from the Perspective of Competition Among Smart Contract Platforms －. https://arxiv.org/abs/2309.11394.

Saito, K. and Yamada, H. (2016). What's So Different about Blockchain? Blockchain is a Probabilistic State Machine. In 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 168.175.

U.S. Securities and Exchange Commission (2024a). Order Granting Accelerated Approval of Proposed Rule Changes, as Modified by Amendments Thereto, to List and Trade Bitcoin-Based Commodity-Based Trust Shares and Trust Units. https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf.

———— (2024b). Order Granting Accelerated Approval of Proposed Rule Changes, as Modified by Amendments Thereto, to List and Trade Shares of Ether-Based Exchange-Traded Products. https://www.sec.gov/files/rules/sro/nysearca/2024/34-100224.pdf.

Wyoming Secretary of State, Business Division (2022). Decentralized Autonomous Organization (DAO): Frequently Asked Questions. https://sos.wyo.gov/Business/Docs/DAOs FAQs.pdf.

SBI 金融経済研究所（2022）.「次世代金融に関する一般消費者の関心や利用度に関するアンケート調査」結果 . https://sbiferi.co.jp/questionnaire/question20221227.html.

————（2024）.「次世代金融に関する一般消費者の関心や利用度に関するアンケート調査、第 2 回」の結果 . https://sbiferi.co.jp/questionnaire/question20240425.html.

金融庁（2024）.「金融商品取引法第二条に規定する定義に関する内閣府令の一部を改正する内閣府令（案）」等に対するパブリックコメントの結果等について . https://www.fsa.go.jp/news/r5/shouken/20240401/20240401.html.