特集《生成 AI・ブロックチェーンと知財》

暗号資産の展開と金融システムへの影響

京都大学公共政策大学院教授　岩下　直行

要　約

暗号資産は世界各国で投資対象として注目を集めており、知財分野においてもその運用に対する関心が高まっている。最近の暗号資産の高騰を受けて、暗号資産が将来、伝統的金融機関の提供する決済サービスにとって代わるのではないか、という予想があるように思われる。現在の暗号資産は匿名で規制を回避して利用できることが評価されているが、脱税や犯罪収益の移転等のリスクを考えれば、無制限な発展を放置することが適当とも思われない。本稿では、暗号資産の技術的基礎、その誕生から現在までの相場変動の経緯と背景を丁寧にたどった上で、将来の展望について考察する。

目次

1．ビットコインの誕生

2008 年、ナカモト・サトシと名乗る正体不明の人物が、ある論文(1)をインターネット上で公表した。それは、インターネット上で利用可能な「電子現金」を作り出し、既存の銀行などに頼ることなく、世界中に資金を送ることを可能にするという提案であった。ナカモト・サトシは、自ら提案を実装したプログラムを 2009 年に公開して協力者を募り、ビットコインの実験が始まった。現在のビットコインは巨額の価値を持つものに変貌したけれど、実験がそのまま継続されているものといえる。

ビットコインは、公開鍵暗号技術によるデジタル署名を利用して権利者の意思を確認しながら、インターネット上での個人間での匿名送金を実現しようというプロジェクトだ。P2P ネットワークを利用し、システム全体を「センターを持たない」形とし、中央組織による情報の独占を防ぐという発想で作られた決済システムである。この理念は革命的であった。安全性、安定性を重視する金融業界においては、決済システムには高機能で高価なセンター・サーバが必要というのが常識だったが、ビットコインは安価なパソコンを使って構築できたからである。

ただし、こうした決済システムが実際に機能するためには、二重使用の問題をクリアする必要がある。紙や金属片を手渡しする現金とは異なり、ビットコインは情報であるため、一度支払いに使用してもその情報は支払った側の手元に残る。その情報が再度利用されてしまうことを有効に取り締まらなければ、実用可能な決済の仕組みとはいえない。

しかし特定の主体が二重使用をチェックする仕組みとすると、「（銀行のような）センターを持たない」という理

念に反するし、それを維持するコストも掛かる。そこでビットコインでは、利用者は誰でもが取引内容を検証できることにした。とはいえ、その場合は二重使用をした者自身が検証者を兼ねてしまい、自らの不正な取引を「正しい」と主張する恐れがある。

そこで検証をしようとする者に特殊な計算（一定の条件を付けたハッシュ値の探索）を行わせ、その作業を最初に完遂した者を信頼できる検証者とする仕組みが考案された。この計算を行うためにはある程度の計算機資源を投入する必要があるが、そのようなコストをかけて検証者になろうとする者であれば、ビットコインの不利益となる二重使用などは行わないという考え方だ。

この特殊な計算によって、ビットコインの開始から延々と連鎖していく新しいブロックが生成される。こうした作業を「マイニング」と呼び、それを行う主体を「マイナー」と呼ぶ。その報酬としてビットコインを新規に発行して与えるという仕組みが考案された。誰が最初に作業を完遂して「発掘」を行い、報酬を手にするかを競い合う仕組みは「競争的マイニング」と呼ばれる。この一連のメカニズムがブロックチェーン技術の原型である。

また、公開鍵暗号によるデジタル署名技術を利用する場合、利用者が秘密鍵と公開鍵のペアを生成し、公開鍵を公開する必要がある。ビットコイン以前は、この公開鍵がどの利用者と紐づくものかを証明するために、認証機関（CA）によるデジタル署名を利用する、公開鍵基盤（PKI）を利用するのが通例であった。しかし、この方式ではPKIを構築するのにコストが掛かるし、「センターを持たない」という思想にも背馳する。そもそも、PKIを構築した時点で、利用者の匿名性が失われてしまう。

そこでビットコインでは、利用者の公開鍵をCAに認証させるのではなく、公開鍵そのものをアドレスとして利用することとした（正確には、公開鍵を2度ハッシュ関数に掛け、そのハッシュ値を英数字にエンコードしたものを利用する）。現在の暗号資産のアドレスとして利用されている30桁程度の英数字の羅列は、こうした経緯で誕生したものだ。このアドレスは利用者の氏名などの情報を一切含まないが、CAを利用しなくてもビットコインの所有者を特定できるし、所有者が公開鍵に対応する秘密鍵を保有していることを立証することも容易である。この工夫によって、第三者の力を借りずに、匿名送金を実現可能となったのだ。

こうしてビットコインは、システムの安定運用と取引内容の検証のための資源を、自給自足で賄えるようになった。「センターを持たない」システムが、どこからも支援を受けず、長年稼働し続けてきたのは、こうした工夫あってのことなのだ。

このようなビットコインの技術的な構造は、情報技術に詳しい人間には特に魅力的に感じられたのだろう。開発された当初は、一般人に知られることはなかったが、パソコンマニアの間のちょっと知的なお遊びとして、ひっそりと実験が続けられていた。

2．ビットコイン前史

ビットコインは電子現金（Electronic Cash）の実現を目指して構築されたものであったが、その誕生以前から、電子現金という構想も、それを実現するための技術（特許）は存在していた[(2)]。例えば、1992年に誕生したSurety社の「Digital Notary」は、ハッシュ値を連鎖させることで電子的なタイムスタンプ性を実現するサービスで、その連鎖の一部のハッシュ値を定期的にニューヨークタイムズ紙に掲載することにより、信頼性を確保するという工夫をしてきた。このサービスは、1990年代以降、実務に活用されてきた実績もある。また、1994年に誕生したDigiCash社の「ecash」は、「blind signature」という暗号技術を使い、取引の匿名性を実現した初めての電子現金である。

また、わが国でも、1996年に、日本銀行とNTTの共同実験により、デジタル署名のチェーンにより転々流通可能な電子現金が開発され、実際に銀行が発行する円建ての電子現金として実証実験が進められた。つまり、ビットコインの誕生前から、ビットコインの特徴である「乱数とデジタル署名を用いた電子現金」「分割可能性、転々流通性、匿名性の付与」「ハッシュ関数や署名の連鎖による改竄防止」について、様々な技術が考案され実装されていたのだ。

1990年代後半から2000年代にかけて、様々な電子現金の提案が行われた。そうした提案の中には、当初は無価

値な電子データを普及させて決済に利用することにより価値を創造しようとした構想も存在したが、全く注目されることなく消滅している。1990 年代から 2000 年代にかけては、利用するコンピュータやネットワーク側のシステムリソースが貧弱かつ高価であったし、インターネット上での電子商取引も普及していなかったから、電子現金が広く普及することはなかった。ecash を発行していた DigiCash 社は、1998 年に倒産してしまった。

これに対して、ビットコインが「成功」したのは何故だろうか。ビットコインもまた、当初は無価値である電子データを決済手段として普及させて価値を創造しようとしている点では、過去に失敗した幾つかの電子現金プロジェクトと同じである。ただし、ビットコインが開発された 2009 年頃になると、CPU、ストレージ、通信のコストが大きく低下しており、個人が趣味でボランティアとして参加するプロジェクトにおいて、十分強力なコンピュータ・リソースが利用可能となっていた。また、オープンソースの文化が普及するようになっていたから、利用者自身がソースコードや取引履歴を検証することで、一定の信頼性を確保することができた。こうした環境において、競争的マイニングという手法を導入することで、システム維持費用の「自給自足」が可能な仕組みを構築できたことが、現在の「成功」の一因と考えられる。

加えて、独自通貨単位（BTC）を採用したことによって、暗号資産が投機・投資の対象と考えられるようになった。新規に決済手段を開発する場合、実際に利用されることを考えれば、法定通貨建ての方が便利だが、それでは交換価値を維持するための費用が掛かってしまう。ビットコインにおいては、システムを支えるマイニングの報酬の分だけ、暗号資産を追加発行することで、外部からの費用投入なしにシステムを維持することが可能になった。実際、ビットコインは、それを管理する法人や組織が明示的には存在せず、誰も責任をもってシステムを維持管理している訳ではないが、開発されてから 15 年間、ほぼ安定して稼働を続けている。こうした実績が積み重なることで、信頼を勝ち得て、無価値であったビットコインを法定通貨と交換する相場が形成され、徐々に価値のあるものとして取引されるようになったのである。

３．ビットコインの相場推移とその背景

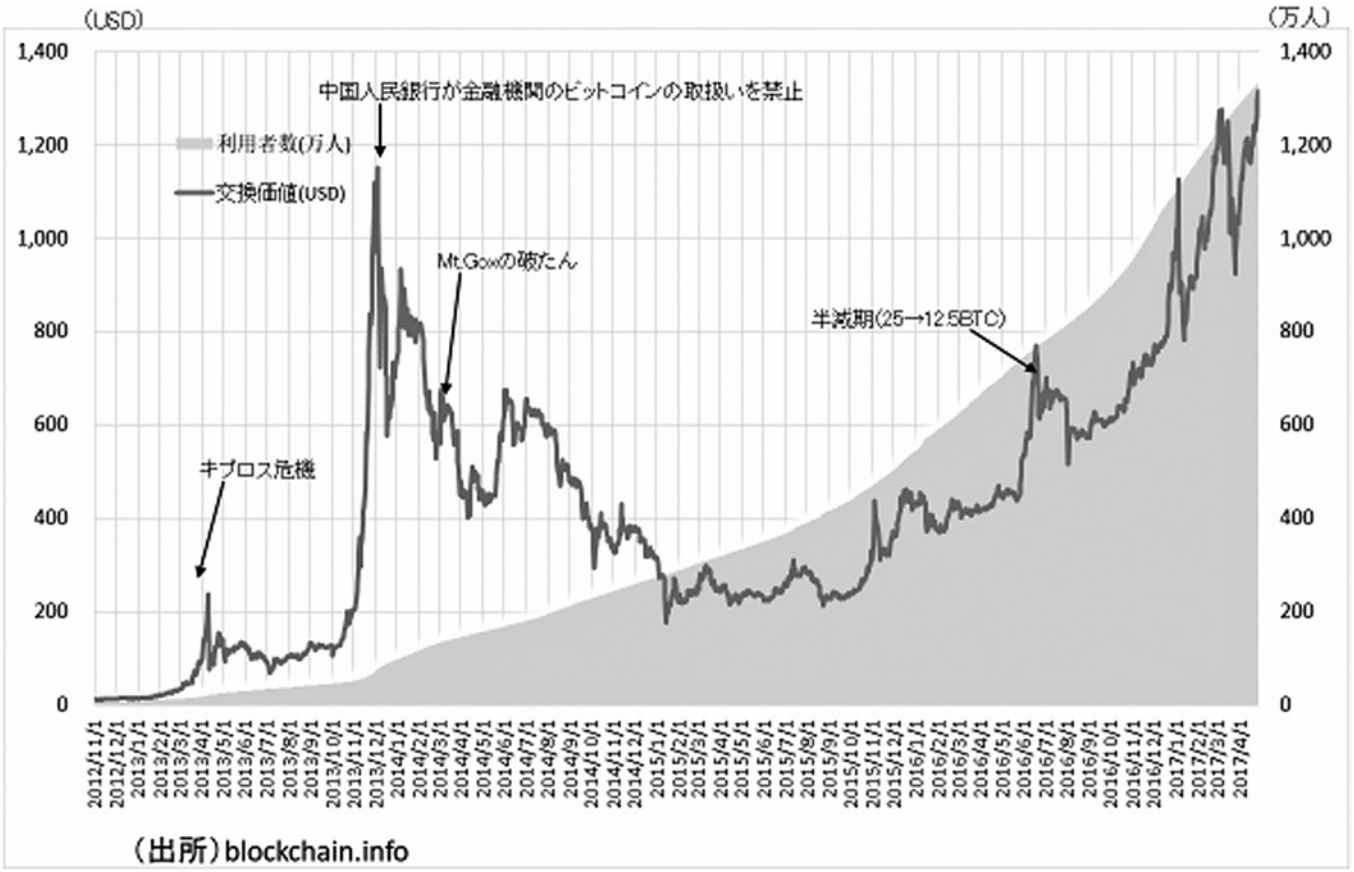
ビットコインは匿名性のある決済手段として開発されたものであったが、それが市場で取引され、法定通貨と交換され、一定の相場が立つようになると、値上がりする投資対象と認識されるようになる。以下では、ビットコインと米ドルとの交換価値（BTC/USD）に着目し、その変動がどのような背景によって生じたのかを時系列を追って解説することとしたい。

３．１　キプロス危機による覚醒（2013-2016 年）

ビットコインは、当初はパソコンマニアの間で注目されていたにすぎないが、徐々に法定通貨と交換されるようになる。当初はほぼ無価値であったが、2012 年頃には 20 ドル /BTC 程度の相場が成立するようになっていた。当時は主として、違法な取引のための匿名送金に利用されるようになっていたらしい。当時の取引の様子は、後に Silk Road 事件として有名になった裏取引サイトを巡る記事に描写されている[(3)]。

ビットコインがマニアのお遊びから、実用性のある送金手段として初めて認識されたきっかけは、2013 年 3 月のキプロス危機であった。地中海の小さな島国、キプロスで金融危機が発生し、一時的に銀行が営業を停止した際に、キプロスから資金を海外に移動させる手段としてビットコインが注目され、実際に送金に利用された。その結果、それまで 20 ドル前後であった相場が、200 ドル近くにまで急騰した。危機が収まると相場は下落したが、この事件を境に国際的な資金移動に利用可能という機能が注目され、ビットコインの相場は更に上昇していく【図表 1】。

次の波は 2013 年末にやってくる。中国国内の電子商取引サイトでビットコインによる支払いが可能になったことを契機に、中国国内での投機熱に火が付いたのだ。相場は過熱し、一気に 1200 ドルにまで値上がりした。こうした相場の過熱を警戒した中国人民銀行は、2014 年初に、中国国内の銀行に対し、ビットコインの購入資金を払い出すことを禁止した。これを主因に相場は一気に半値の 600 ドルに暴落する。更に、当時日本に存在した世界最大手の暗号資産交換所、Mt.Gox 社の破綻が重なって相場は下げ基調となり、2015 年頃には再び 200 ドル近くに下



図表１　ビットコインの価格と利用者数の推移（2013～17 年）

落したが、2017 年初頭には再び 1000 ドル前後の水準に戻った。

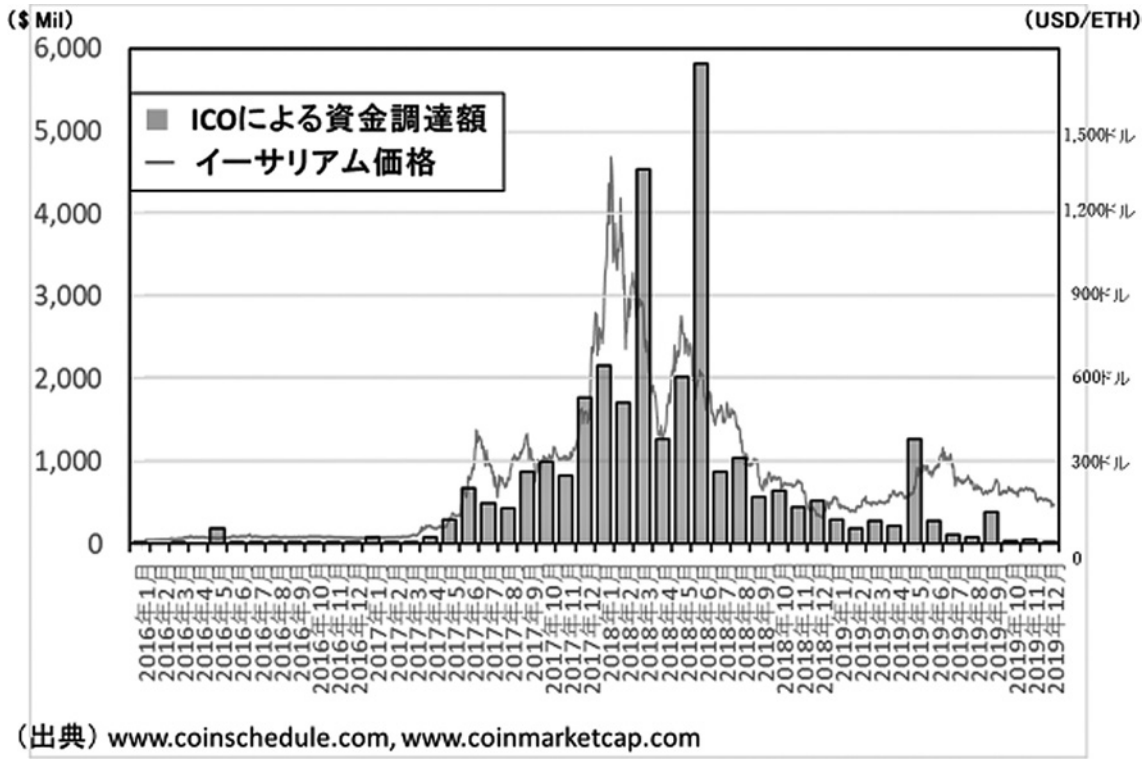
３．２　ICO ブームを受けた高騰（2017 年）

2017 年に入ると、ビットコインの相場は急速な高騰をみせる。2017 年 1 月は 1,000 ドル程度で推移していたが、2017 年 12 月の最高値は 20,000 ドルと 20 倍近い値上がりとなった。相場が大台を超える都度、マスコミが大きく報道し、世間からの注目度も高まっていった。

暗号資産の 2017 年の相場高騰の原動力は、ICO（Initial Coin Offering）であったと考えられている。ICO とは、「企業等が電子的にトークン（証票）を発行して、公衆から資金調達を行う行為の総称」である。世界中で行われた ICO は、2017 年に 6.6 億ドル、2018 年には 21.6 億ドルに拡大した。

ICO の大半は、暗号資産イーサリアムを基盤に利用し、ERC-20 と呼ばれる標準を利用した新しい暗号資産（トークン）が発行される。この購入にはイーサリアムが必要になるので、ICO が増えると、イーサリアムの需要が増え、相場が上昇する。また、ICO で発行されたトークンは払込金を償還するようなものではないのだが、イーサリアム建てで発行されるから、イーサリアムの相場が上昇すると、トークンのドル建て価格は上昇する。その結果、トークンの流通市場での価格が高騰し、それが更なる ICO の活性化をもたらす。このような正のフィードバックが働いて、ICO の発行が急増した 2017 年 5 月を起点に ICO 発行額とイーサリアムの相場が急騰することとになったと考えられる【図表 2】。

ビットコインは「未来のお金」であり、決済に使えるのでは、という期待から、高値が続いていた。イーサリアムは、ICO の基盤として急激に値上がりした。この 2 種類の暗号資産が値上がりすると、それ以外のコインも、第二、第三のビットコイン、イーサリアムとして、値上がりが期待されることになる。それまでほぼ無価値であった多くのコインが、一斉に値上がりを始めたのが、同じく 2017 年 5 月であった。そうした動きは、ある程度名の知られたコインが一通り買われて値上がりすると、知名度が低く価格も付いていないようなコインに値上がりが伝播していく。こうして、2017 年に様々な暗号資産が値上がりしたのだ。



図表２　ICO による資金調達額とイーサリアム価格の推移

３．３　コインチェック事件とビットコインの冬（2018-2019 年）

2018 年入り後、暗号資産の市況は調整局面に入った。ビットコインの価格も、全暗号資産の流通総額も、わずか１か月程度でピーク比の 1/3（価格：7000 ドル）にまで下落した。その後も相場は弱含みで、2019 年２月まで下落を続け、ビットコインの価格が 3400 ドルにまで低下した。この相場低迷期は、「ビットコインの冬」と呼ばれる。

相場下落は急上昇の反動によるものであったが、暴落の直接的なきっかけとなったのは、コインチェック事件である。2018 年１月、日本の大手暗号資産交換業者であるコインチェック社から、時価 580 億円相当の暗号資産 NEM が盗まれてしまった。何者かが同社の管理するデジタル署名用の秘密鍵を不正に利用して、同社が保有していた NEM を全て他のアカウントに移動させたのである。コインチェック社は、セキュリティ対策が不十分であったことを認め、顧客に補償したが、長期間の営業停止を余儀なくされ、２度にわたる金融庁からの業務改善命令を受けることとなった。

そもそも暗号資産交換業者は、ビットコインが高騰した 2013 年以降、多くの素人投資家が市場に参入したために誕生したビジネスである。彼らの仕事は２つあった。法定通貨と暗号資産を交換すること、交換した暗号資産を預かることだ。現在では、暗号資産を交換業者から購入すると、交換業者の保有するアカウントに保管され、投資家の氏名と残高が、取引所の RDB に記録されるシステムが一般的となっている。素人の投資家は、それまでの投資家であるパソコンマニアとは違い、安全に秘密鍵を管理、運用することができなかったから、交換業者がその代役を果たすことになったのだ。

その結果、暗号資産の取引には、従来のオンチェーン取引に加えて、オフチェーンオフチェーン取引が行われるようになった【図表 3】。オンチェーン取引では、利用者がデジタル署名のための秘密鍵を管理し、その署名の真正性によって取引を認証する。オンチェーン取引は、主に暗号資産の取引に習熟している専門的な投資家によって用いられる。blockchain 上にその利用者のアドレスによる取引記録が書き込まれるので、オンチェーン取引と呼ばれる。これに対し、オフチェーン取引は、暗号資産を交換業者が管理し、利用者からの売買の指示は ID とパスワードで行う仕組みだ。具体的な統計はないが、投資家の人数の上では大多数を占める一般の投資家が自ら電子署名の秘密鍵を管理することは難しいし、サイバー攻撃のリスクを考えれば危険でもある。このため、今日では、暗号資産投資家のほとんどはオフチェーン取引を行っていると考えられる。

図表３　暗号資産取引の２つの類型

類型	オンチェーン取引	オフチェーン取引
概要	ビットコインの黎明期から続けられてきた取引方法。利用者が自ら管理する秘密鍵でデジタル署名を生成し、自らのアドレスを含む取引記録がブロックチェーンに記録され、ブロックが伸延すれば書き換えが事実上不可能になる。	2013 年頃から増えてきた暗号資産の交換業者を利用する取引方法。暗号資産は交換業者名義のまま、交換業者の RDB で振替決済を行う。利用者は秘密鍵やアドレスを持たず、ID、パスワード等で認証する。
利用者	ビットコイン黎明期に参加した愛好家、匿名による取引を希望する利用者、国境を跨いで送金・支払をする利用者、取引所間取引、採掘業者	暗号資産取引については素人である個人投資家、暗号通貨の交換業者の顧客
メリット	取引がブロックチェーンに書かれるので取り消されることがない。（ほぼ）匿名での取引が可能。仮に交換業者にトラブルがあったとしても、ブロックチェーンに記録された暗号資産は安全。	投資家自らが秘密鍵を管理する必要がなく、秘密鍵の紛失や漏洩の被害を受けない。パスワード等の簡便な認証手段で取引できるため、素人でも取引できる。
デメリット	利用者自らがデジタル署名の秘密鍵を安全に管理する必要があるため、技術に詳しい必要。秘密鍵の紛失や不正利用があれば、暗号資産を失う。	取引は交換業者の RDB に書かれるだけなので、交換業者だけが頼り。サイバー攻撃等で交換業者が被害を受けると、資産を失うリスクもある。

投資家にしてみれば、オフチェーン取引は手続きが簡単なだけでなく、秘密鍵の安全な管理という責任の伴う難しい操作を交換業者に丸投げできるという意味で、暗号資産の取引を容易にするものであった。これに対し、大勢の素人の投資家から大量の暗号資産を預かる交換業者には、大きなリスクが溜まっていった。暗号資産の価格高騰もあって、交換業者が日々取り扱う金額はどんどん高額になっていった。そのような肥大化した交換業者が、サイバー攻撃の犠牲となった。暗号資産のビジネスはまだ生まれて時間が経っておらず、交換業者はベンチャー企業ばかりであり、残念ながらそのリスク管理の水準は高くはなかった。世界各国の交換業者がサイバー攻撃のターゲットとされた。

攻撃者の側からみれば、攻撃対象のシステムの多くはクラウド上に構築され、秘密鍵を含めてリモート運用されているものも多い。交換業者を狙ってサイバー攻撃を仕掛けて、その秘密鍵を不正に利用すれば、巨額の暗号資産を自らの管理するアカウントに移動させることができる。一旦移動させてしまえば、匿名で送金できるという暗号資産の特徴を悪用して、資金洗浄も自由自在である。その意味で、攻撃者にとって交換業者のシステムを狙うという行為は、極めて合理的な判断であったのだ。

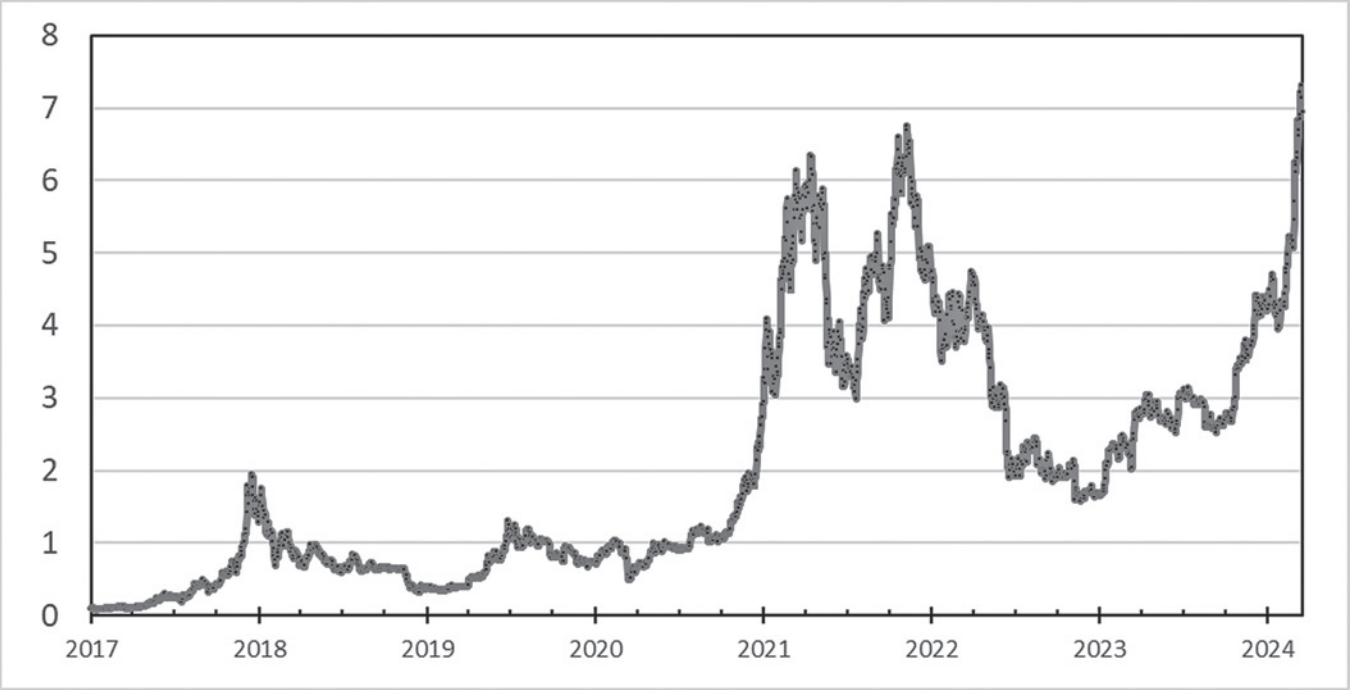
これに対して、顧客の大事な資産である暗号資産を預かる立場として、交換業者の体制は不十分であった。世界中で、交換業者がサイバー攻撃を受け、顧客から預かった暗号資産を奪われるという事件が続発した。攻撃者は特定されることは困難で、奪われた殆どの暗号資産は取り戻されていない。

３．４　コロナショックによる暴落からの再高騰（2020-2021 年）

2019 年に若干持ち直したビットコインであったが、2020 年から 2021 年にかけて、ビットコイン相場は再び大きく変動する。コロナショックを受けて 2020 年 3 月に 10,000 ドルから 5,000 ドルへと暴落したのだ。しかし、その後、株式相場と歩調を合わせて急速に値を戻す。2020 年後半からは過去にない急騰を示し、2021 年 11 月には 67,000 ドルに達した【図表 4】。

2020-21 年の暗号資産相場における特徴的な動きとしては、ビットコイン相場の主要国株価との連動の高まりが挙げられる。2017 年の相場高騰時には、暗号資産のみが急上昇し、主要国の株価が特に高騰したわけではなかった。当時、株価とビットコインはまったく連動しない資産と言われていた。これに対し、2020-21 年の暗号資産相場は、主要国の株価指数と動く方向が一致している。

2020 年初頭、コロナ感染症のパンデミックの結果、世界経済は大恐慌以来といわれる深刻な縮小を余儀なくされた。2020 年 3 月には、実体経済の落ち込みが資産価格を低下させるのでは、という懸念が広がり、主要国の株価が暴落した。これに対し、主要国の金融当局は、実体経済の危機を金融危機に繋げることのないよう、一斉に金



出所：CoinMarketCap

図表 4　ビットコインの価格の推移（2017–2024 年）

融緩和の度合いを強めた。財政当局も、財政赤字の拡大を甘受して、国民への支援に努めた。こうした政策対応の結果、主要国の株価は持ち直し、その年の内に、多くの国で株価指数が史上最高値を更新した。また、日本の株価指数も上昇を続け、2021 年 2 月には日経平均は 3 万円を超え、1990–91 年の株価バブル崩壊以降では最も高値を付けた。

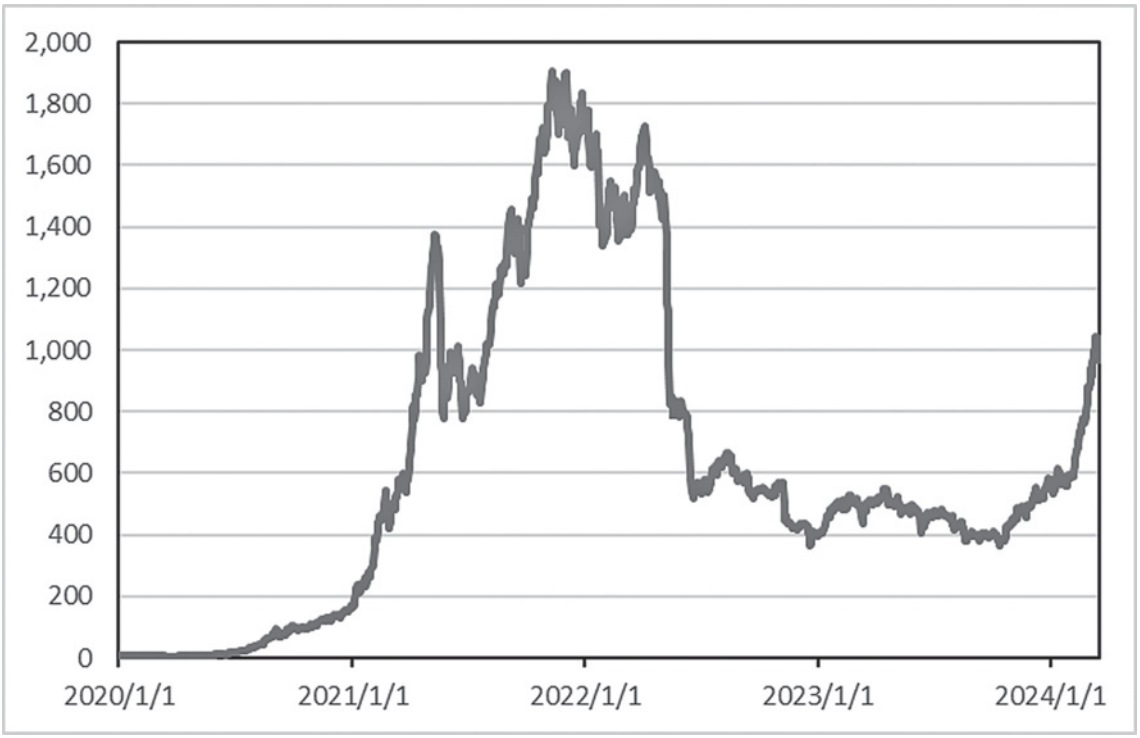
コロナ感染症の不安が横溢する中での 2020 年 3 月の株価暴落は、金融当局としては放置しておけないものであったから、金融当局の対応は妥当なものであっただろう。もちろん、そうした政策対応は、決して暗号資産相場の下落を意識して行われたものではなかった。金融危機回避のための金融緩和強化のいわば副作用として、暗号資産が高騰してしまったといえるだろう。

暗号資産ビジネスの形態の観点からみると、2021 年の相場上昇の原動力となったのは、分散型金融（DeFi：Decentralized Finance）と呼ばれる新しいスタイルの暗号資産取引の流行であったと考えられる。DeFi では、DEX（Decentralized EXchange）と呼ばれるネット上の仮想取引所で、暗号資産の売買、貸借の仲介、ステーブルコインの発行などが行われている。これらの取引はスマートコントラクトによって実行され、暗号資産のエコシステムの中で、自律的に作動すると説明されている。同時に、これらの取引のために利用される DeFi トークンと呼ばれる暗号資産が拡大している。それらのスマートコントラクトに取り込まれた暗号資産の価値（TVL：Total Value Locked）は、2020–21 年に急速に拡大している【図表 5】。

DeFi が拡大する中で実際に起きているのは、2017 年の ICO トークンのブームと似た現象である。DeFi の活動開始時には「ガバナンス・トークン」と呼ばれる新たなトークンが発行され、それらも高騰している。ICO トークンに比べると説明がやや洗練されてはいるが、実態はあまり変わらない。かつての ICO プロジェクトの中には、DeFi と同様の構想を唱えるものもたくさんあり、その多くは失敗してトークンは無価値になっている。ICO も DeFi も、トークンとしては ERC-20（イーサリアムブロックチェーンのトークン規格）を採用することが多いが、ICO トークンが相次いで値下がりし、投資家から信頼を失ったために、DeFi に名を変えて再登場させたという見方も可能であろう。

３．５　欧米の金融引締めによる相場暴落と市場の混乱（2022 年）

2021 年 11 月、米国 FRB が量的緩和の縮小を決定し、世界的な超金融緩和に終止符が打たれた。ほぼ同時に、



出所：DeFiLlama

図表 5　DeFi 市場の TVL（Total Value Locked）の推移（2020-2024 年）

それまで高騰を続けていた暗号資産相場が暴落する。ビットコインの対ドル相場は、2021 年 11 月に記録した 67,000 ドルから、2022 年 1 月には約半値の 36,000 ドルとなり、2022 年 11 月には約 1/4、16,000 ドル前後に下落した。

2022 年に暗号資産相場が暴落したのは、米国と欧州における金融政策の変更の影響を受けたものだ。世界的なインフレの進行を受け、米国と欧州の中央銀行が相次いで政策金利を引き上げた。コロナ感染症のパンデミックに対処するために 2020 年 3 月から進められてきた世界的な金融の量的緩和は終了し、欧米はインフレに対応するための金融引締め期に入った。

金融政策の変更は、好調に推移していた各国の株価指数にも影響を与えた。ただし、大手製造業、金融などの優良企業は収益が好調であるため、その株価は金利上昇のダメージをあまり受けていない。これに対して、相対的に収益や配当が少なく、金利変動に敏感な新興企業の株価は大きく下落した。暗号資産は配当などの利益を生まないため、金利上昇局面では新興企業の株価以上に暴落することになった。

2022 年の暗号資産相場の下落は、暗号資産市場を舞台に展開されていた不透明なビジネスの問題点をあぶり出すことになる。5 月にはステーブルコイン UST の崩壊という事件が起き、11 月には米国の大手暗号資産交換業者 FTX 社が破綻した。UST 事件と FTX 事件は、更なる暗号資産市場の混乱、相場下落、連鎖的に発生した関連企業の倒産を引き起こした。

UST 事件：　ステーブルコインとは暗号資産の一種で、1 コイン =1 ドルという価格が維持されると発行体が宣言したものである。暗号資産市場と伝統的な金融市場との間には一種の障壁があるため、暗号資産投資家が銀行預金で決済を行おうとしても、タイムリーに取引できない。価格が 1 ドルで安定している暗号資産であるステーブルコインを決済手段として利用すれば、例えば相場上昇時に迅速に利益確定ができる。そうした用途のために、2017 年頃から自然発生的に様々なステーブルコインが発行され始め、現在では総発行額は 1,000 億ドルを越えて拡大している。

発行体は、価格が 1 ドルで安定する根拠として、発行額と同額以上の米ドル建て安全資産を保有しているとか、発行額よりも十分多い暗号資産を保有しているなどと説明し、投資家を安心させようとする。しかし、いずれも規制当局のチェックを経たものではなく、信頼できるとは言い難い。こうした中で、2021 年 11 月から急速に発行を拡大したステーブルコインが UST であった。UST は 2022 年 5 月に 180 億ドルにまで発行額を拡大した後に暴落

した。1UST=1ドルの価格を維持できず、ほぼ無価値となった。価格が維持されると信じてUSTを購入した投資家は、大きな損失を被り、暗号資産市場は大混乱することとなった。

FTX事件：　2022年11月、米国の大手暗号資産交換業者FTX社が破綻し、百万人の顧客が同社に預けていた暗号資産を引き出せなくなった。FTX事件は、その規模の大きさ、被害者の人数の多さなどから、暗号資産市場で過去に発生したトラブルと比べても、深刻度の高いものであった。暗号資産交換業者は、単に暗号資産の売買を仲介するだけではなく、購入した暗号資産を顧客に代わって自分名義で預かるという役割を持つ。通常の金融機関に当てはめれば、売買の仲介までは証券会社と似ており、それを預かるところは銀行と似ている。日本では、コインチェック事件の反省から交換業者への規制・監督が強化されており、万一破綻しても顧客資産が守られるための工夫が講じられているが、米国ではそうした規制が緩く、FTX社の杜撰な経営が放置されていたことも、事態を深刻化させた。

2020-21年の相場高騰により、米国では、通常の機関投資家の間でも、暗号資産取引に関与する先が増えていた。その多くはプライベート・エクイティ・ファンドなどを経由して投資するのだが、そうしたファンドの多くも、FTX事件に巻き込まれることとなった。投資ファンドといえども、暗号資産取引の専門家ではないから、自らが秘密鍵を管理するオンチェーン取引ではなく、FTX社に資産を預けるオフチェーン取引で投資していたとみられる。暗号資産は値動きが大きいため、ある程度のリスクは覚悟して投資していたのであろうが、資産を預けたFTX社が破綻し、資産を引き出せなくなることはさすがに想定外であった。

３．６　金融緩和期待を受けての相場上昇（2023-2024年）

2023年に入ると、ビットコインの相場は底を打ち、急速な上昇に転じた。2023年初に16000ドル台で低迷していた相場は、1年を超えて上昇を続け、2024年3月には史上最高値を更新して73000ドルに到達した。この高騰は、一見すると2022年の暴落からの自然な反動に思えるかもしれない。しかし、詳細に見てみると、これまでのパターンから外れた特殊な現象だと言える。

まず、2023年は世界的に金融引締めが強化された年であり、日本を除けば、主要国の中央銀行は軒並み政策金利が高い状態を維持していた。2009年のビットコインの誕生以来、世界的な金融緩和が続くなかで暗号資産は高騰したため、多くの金融市場関係者は、暗号資産の価格上昇を低金利の下で発生したバブルの一種と見なしていた。その意味では2022年に多くの国で金利が上昇し、暗号資産が暴落したところまでは理解できる範囲であった。しかし、2023年には、高金利が続く中での相場上昇という、従来とは異なる局面を迎えたのである。

2023年は日米欧で世界的な株高が進行しリスク資産が値上がりしたため、暗号資産が値上がりしたこと自体は不思議ではないようにも思える。しかし、株価のベースとなるのは企業収益である。2023年に先進主要国の株価が上昇した背景には、物価上昇局面において製品価格が生産要素価格（賃金など）よりも先行して上昇した結果、企業収益が好調であったことが挙げられる。ところが、暗号資産に投じられた資金が経済活動を通じて収益を生み出す仕組みは存在しないから、株価の上昇と同列視はできない。

暗号資産の過去の値上り局面を振り返ると、2017年はICO（Initial Coin Offering、新規の暗号資産公開）が世界的に流行し、錬金術的な資金循環ビジネスを誕生させたことが相場高騰のエンジンとなった。2020～2021年は、コロナ対策の金融緩和拡大に加え、NFT（Non-Fungible Token）やDeFi（Decentralized Finance）といった新しいビジネスが活性化したことが相場上昇に繋がった。しかし、2023年の暗号資産の高騰は、暗号資産本体に限られ、ICO、NFT、DeFiといった派生分野は活性化していない。つまり、暗号資産が新しい金融商品や投資機会を誕生させたから値上がりしているわけではないのだ。この点からも、2023年の高騰はこれまでのパターンから外れた現象といえる。

2022年の暴落においては、ステーブルコインの価値喪失（UST事件）や最大手交換業者の破綻（FTX事件）など、暗号資産業界で長年懸念されていたリスクが顕現化し、隠蔽されていた不透明なビジネスの実態が暴かれることになった。2023年になると、悪材料が出尽くした結果、相場が上昇に転じたともいわれている。こうした説明は株式市場などでもよく聞かれるのだが、問題は、隠蔽されている不透明な取引慣行が透明になったとも、潜在

的なリスクが解消したともいえないことだ。

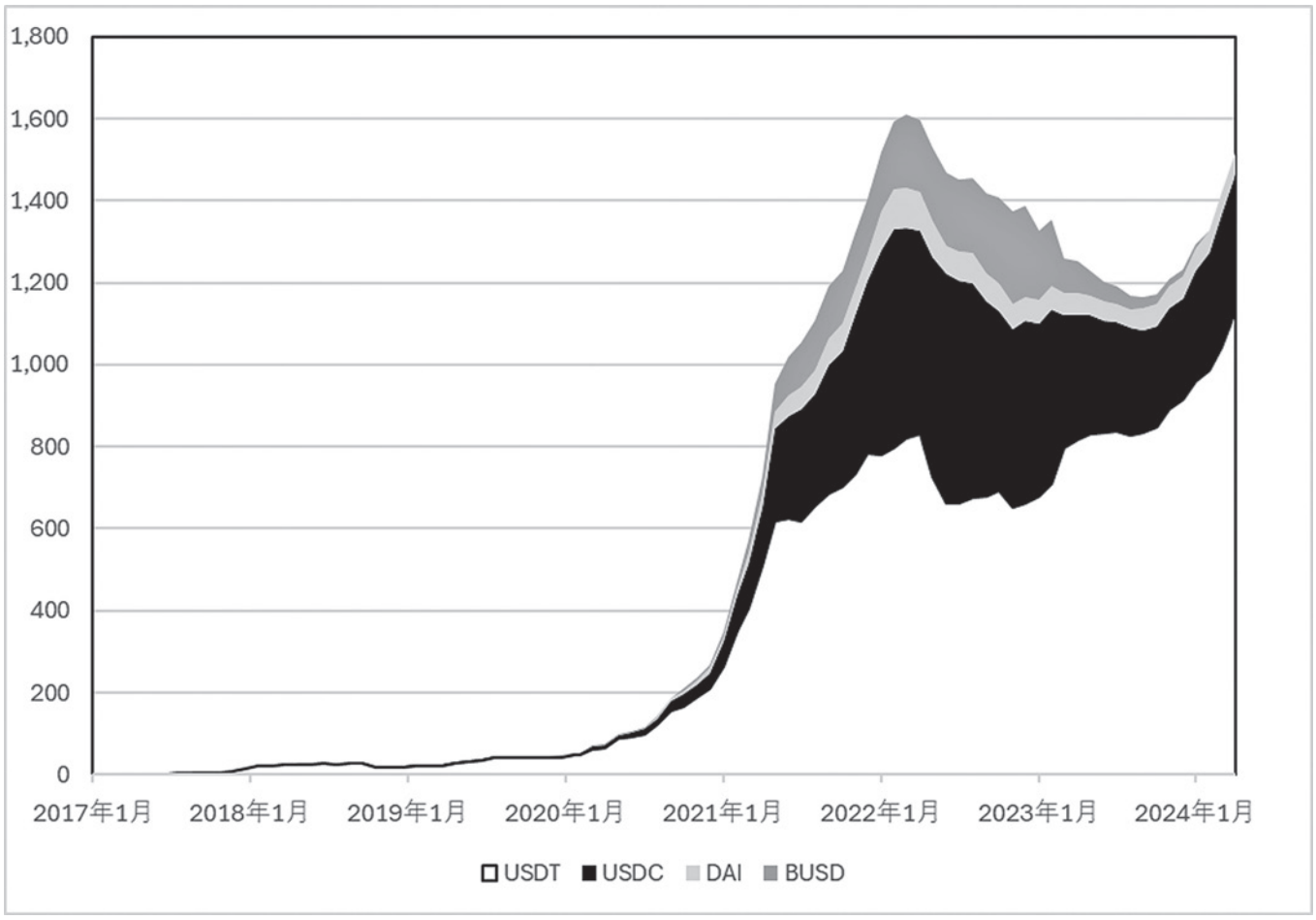
そんな中で、ビットコイン相場の上昇の材料とされたのが、米国におけるビットコイン ETF（上場投資信託）の認可である。2024 年 1 月には認可が近いことが囁されて相場が急上昇したが、実際に認可されたとの報道でむしろ相場は下がった。

その後は、2024 年 4 月のビットコイン半減期が材料として囁された。半減期とは、ビットコインの採掘報酬が半分に減少することで、ビットコインの新規供給が減少するから相場上昇に繋がるというロジックらしい。しかし、そもそも 4 年毎に報酬が半減するのはビットコインの発行総量が 2100 万 BTC にとどまるという計画の一部を構成するものだ。予定通りに変更が実施されるから相場が上昇するという説明は説得的ではない。暗号資産業界は、今後もこうした「囃す材料」を探し続けるのだろう。

４．暗号資産市場と伝統的金融市場との境界

世界各国では、現在、暗号資産に関する規制が急ピッチで整備されつつある。規制が整備されて業界が浄化されれば、暗号資産市場と伝統的な金融市場との垣根が低くなり、伝統的な金融市場に滞留している資金が暗号資産市場に流入することが期待されるという声も多い。その最たる例がビットコイン ETF の導入であり、期待通りに相場が高騰したと解釈できる。とはいえ、新旧の市場間にある垣根を低くすることに伴う弊害やリスクはないか、今一度慎重に検討する必要があるだろう。

特に注目されているのは、ステーブルコインである。その発行残高は暗号資産の高騰に合わせて増加していたが、2023 年以降の相場高騰局面では、むしろ発行残高は若干減少していた。特に、USDC（USD Coin）と BUSD（Binance USD）の落ち込みが激しい【図表 6】。



出所：CoinMarketCap

図表 6　ステーブルコインの発行残高の推移

USDC は、2023 年 3 月のシリコンバレー銀行の破綻の際に、発行コインの裏付け資産として同銀行への預金を大量に保有していた。破綻報道が流れた際に、大口預金者の預金が払い戻されないリスクが指摘され、USDC は一時的に 1 コイン＝ 1 ドルのペッグを失った。最終的に、同銀行の預金は全額保護されたが、市場の信頼と安定性が損なわれたことから USDC は大きくシェアを失うこととなった。結果、1 年間で発行残高はほぼ半減した。

BUSD は、2023 年に発行額を 9 割以上減少させた。これは、BUSD の発行主体の 1 つである暗号資産取引所バイナンス（Binance）の不正行為が原因であった。2023 年 6 月、米証券取引委員会（SEC）はバイナンスと同社 CEO チャンポン・ジャオ氏（当時）を米国証券法違反の疑いで訴えた。11 月に同社とジャオ氏は米国で事業を継続するために司法取引に応じ、罰金 43 億ドルを支払い、マネーロンダリングへの関与を認めたジャオ氏は CEO を退任した。この結果、バイナンスはステーブルコイン事業を続けていくための信任を維持できないと判断し、BUSD のサポートを段階的に終了することを発表した。また、新しい BUSD トークンの発行は停止された。

こうした中で、最大の発行残高を占める USDT（テザー）は、むしろ発行額を増やし、シェアを大きく上昇させている。とはいえ、USDT を発行するテザーやその関連企業である香港のビットフィネックスも、USDT を巡って米国の司法当局から指摘を受けた経緯もあり、潜在的なリスクは大きい。USDT は、ロシアに対する経済制裁を逃れるために利用されているとの報道(4)もある。

そもそも、ステーブルコインは発行主体の実質的な負債であるにもかかわらず、銀行規制や証券規制の対象とされていない。

2022 年の UST 事件で明らかになったのは、暗号資産市場においてもドル建て価格を保証する資産として提供するのであれば、それらは一般の通貨と同じくその発行額を負債とする主体への信任が必須ということだ。今のところ、暗号資産の世界に閉じているという前提で、USDT のようなステーブルコインは各国の規制対象となっていない。これは暗号資産の世界と伝統的な金融の世界との間に垣根があり双方とも他方に侵入しないことを前提としているためだ。しかし、世界各国で暗号資産に関する規制が急ピッチで整備されつつあるなかで、今後もそのような前提が引き続き成り立つのか、慎重に見極めていくことが必要であろう。

（注）

(1) Nakamoto, Satoshi, “Bitcoin：A Peer-to-Peer Electronic Cash System”

(2) 当時議論されていた技術の内容とその特許法上の位置付けについては、岩下直行・相澤英孝、「電子マネーを取り巻く状況と特許法」（相澤英孝編『電子マネーと特許法』、弘文堂、2000/07/15）を参照のこと。

(3) Bearman, Joshuah, “SILK ROAD：THE UNTOLD STORY,” https://www.wired.com/2015/05/silk-road-untold-story/

(4) ウォールストリートジャーナル記事、「ロシアの兵器部品密輸、仮想通貨で制裁逃れの内幕」（2024 年 4 月 5 日）
https://jp.wsj.com/articles/inside-the-russian-shadow-trade-for-weapons-parts-fueled-by-crypto-27651a7e

（参考文献）

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

(2) Chaum, D.：“Blind Signatures for Untraceable Payments,” Advances in Cryptology Proceedings of Crypto. 82.

(3) Okamoto, T. and K. Ohta, “Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility,” Advances in Cryptology – EUROCRYPT'89, LNCS 434, pp. 134-149, Springer-Verlag, 1989

(4) Bearman, J：“SILK ROAD：THE UNTOLD STORY,” https://www.wired.com/2015/05/silk-road-untold-story/

(5) 相澤英孝編、『電子マネーと特許法』、弘文堂、2000/07/15

(6) 岩下直行、「暗号資産への脅威と対策―ビットコインの社会への展開による変質―」、情報処理学会デジタルプラクティス 10（3）、pp.441-456、2019 年 7 月 15 日

（原稿受領 2024.4.30）