

# 暗号資産の現在と将来

応  
般



岩下直行 | 京都大学

最近の暗号資産の値上がりの背景には、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、という期待があるように思われる。暗号資産への注目の高まりを反映して、各国では中央銀行デジタル通貨の発行が検討されており、いくつかの国では実際に試行が始まった。しかし、暗号資産は既存の金融機関を代替するものではなく、脱税や犯罪収益の移転、テロ資金供与のリスクも考えれば、その無制限な発展が今後も放置されるとは考えにくい。本稿では、さまざまな視点から暗号資産の現在と将来について検討し、そのインパクトについて解説する。

## ビットコインの誕生

暗号資産の歴史は、2008年にナカモト・サトシを名乗る正体不明の人物が2008年にビットコイン論文<sup>1)</sup>を公表し、2009年に最初のバージョンを公開したのを嚆矢とする。それは、インターネット上で利用可能な電子現金を作ろうという野心的な実験であった。

ビットコインは、電子情報に公開鍵暗号技術によるデジタル署名を付与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。

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2～3年間は、一般の人々から注目されることはなかったが、パソコンマニア (geek) 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。

ビットコインの誕生以前から、電子現金という構想も、それを実現するための技術は存在していた。たとえば、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 closed-loop 型の電子現金である。また、我が国でも、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、「乱数とデジタル署名を用いた電子現金」「分割可能性、open-loop 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、さまざまな技術が考

案され実装されていたのだ。

しかし1990年代から2000年代にかけては、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」したのはなぜだろうか。

ビットコインが開発された2008～2009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していたから、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。

誰も責任を持ってシステムを維持管理しているわけではないが、開発されてから12年間以上、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、徐々に信頼を勝ち得て、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。

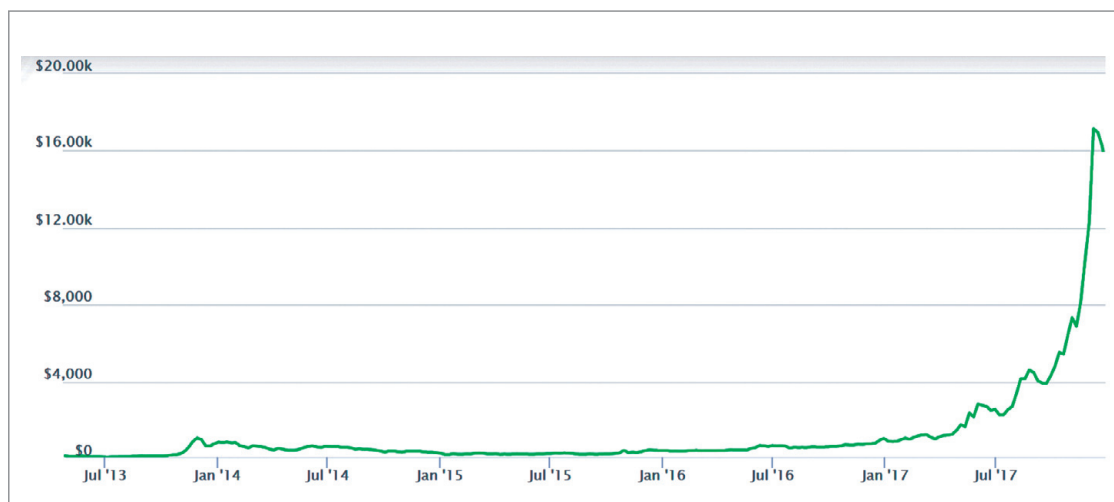
## ビットコインの相場推移 (1) ICOブームを受けた2017年の高騰

ビットコインが実用性のある投資対象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。キプロスで金融危機が発生し、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送金に利用された。とはいえ、当時の相場は200ドル程度にすぎなかった。

ビットコインが大きな注目を集めたのは、2017年であろう。年初は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(図-1)。

2017年のビットコインの大相場をどう理解すればいいのだろうか。暗号資産市場全体に占めるビットコインのシェアは、85%から40%弱へと半減した(図-2)。

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<sup>2)</sup>」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が増えると、イーサリアムの需要が増え、相場が上昇する。その結果、ICOの発行が急増した2017年



■ 図-1  
ビットコインの  
価格の推移  
(2013～2017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になったと考えられる(図-3)。

ビットコインとイーサリアムが値上がりすると、それ以外の暗号資産も値上がり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暗号資産が、一斉に値上がりをはじめたのが、同じく2017年5月であった。株式相場が上昇基調にあるときの、「低位株の循環物色」のような現象が発生したのだ。これが、2017年にアルトコインが高騰したメカニズムであり、それがビットコインの相場も引き上げ

たとえられる。

## ビットコインの相場推移(2) コロナ環境下における再高騰

ビットコインの相場は、2018年の暴落後の「ビットコインの冬」の時期を経て、しばらく低迷するが、2019年には1万ドル前後の相場を取り戻していた。その後、2020年3月のコロナショックで一時的に5,000ドルにまで下落するが、その後再高騰し、

2021年4月には既往ピークの6万4千ドルを記録した(図-4)。

ビットコインはなぜ再び値上がりしたのだろうか。2020年に、ビットコインへの投資家行動が、それ以前と比べて大きく変化したとは考えにくい。かつては、「未来のお金」と囃されたものの、実際には通貨としては利用できないものであることは広く知れ渡ってしまった。投資家の顔ぶれを見ても、海外ではプライベート・エクイティなどのファンド筋が投資していると言われているが、伝統的な金融機関や大手の機関投資家は、引き続き暗号資産への投資を見送っている。暗号資産に投資しているのはセミプロを含む個人投資家が主体であることは変わらない。

2020年の後半から異様な伸びを示している計数が存在する。分散型金融(Decentralized Finance: DeFi)と呼ばれる新しいスタイルの暗号資産の取引が活発化しており、暗号資産の売買や貸借の仲介、ステーブルコインの発行等が行われている。といって

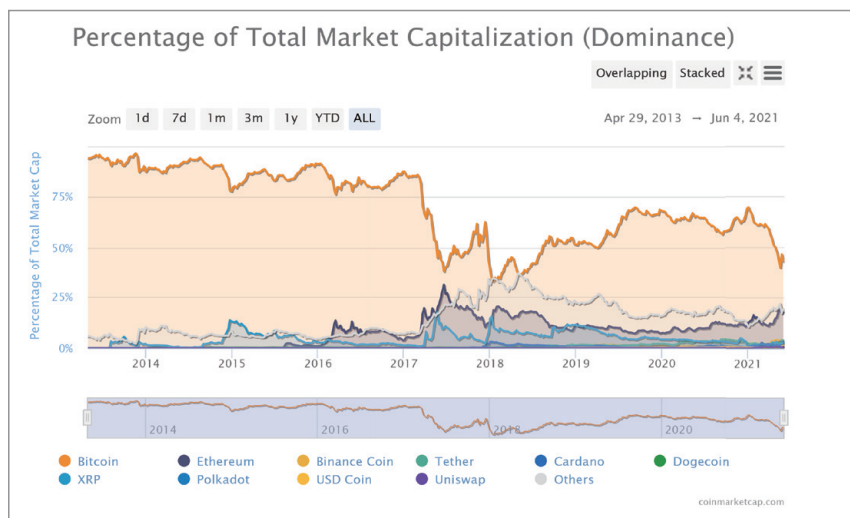


図-2 暗号資産の種類別流通総額の構成比の推移(2013~2021年)

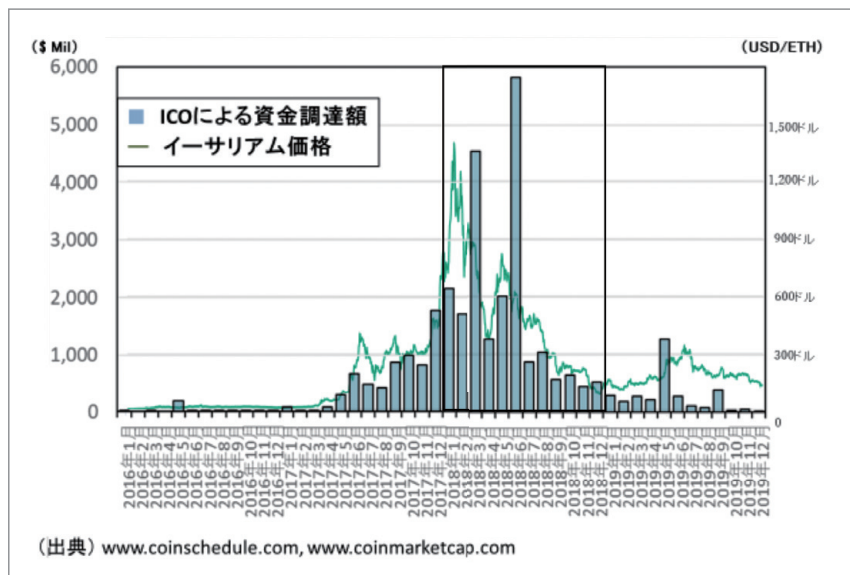


図-3 ICOによる資金調達額とイーサリアム価格の推移



も、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、自律的に作動していると説明される。そして、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の流通残高が急拡大している (図-5)。

ICO は 2017 年から 2019 年にかけて、300 ～ 400 億ドルを調達したと言われていたが、DeFi トークンの流通総額はわずか数カ月で 1,500 億ドルに達しているから、その規模はすでに ICO を凌駕している可能性が高い。DeFi トークンはきわめて短期間に普及し値上がりしたため実態が十分に知られていないが、今後の展開を注視する必要があるだろう。



図-4 ビットコインの価格の推移 (2017～21年)

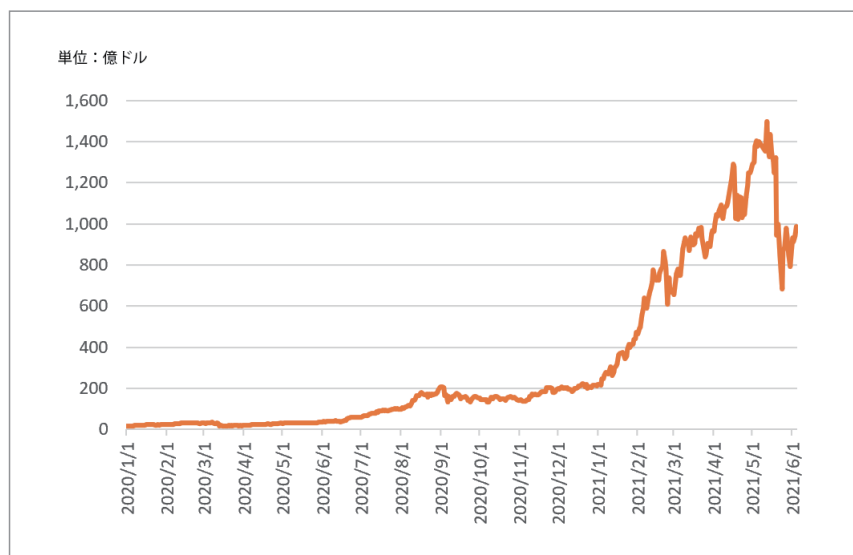


図-5 DeFi トークンの流通総額の推移 (2020～2021年)  
(データ) Top 100 DeFi Coins by Market Capitalization (<https://www.coingecko.com/>)

## 暗号資産に対する伝統的な金融業界の受け止め方

暗号資産に対する伝統的な金融業界の人間、たとえば銀行員や証券マンなどの反応は、概して冷淡であることが多い。以下では、その背景について考えてみよう。

ビットコインが誕生してから、その価格がどのように生成されるのかについては、さまざまな言説が見られる。基本的に暗号資産を伝統的な金融商品である株式や公社債と類似のものだと位置付けるならば、価格は資産が稼ぎ出す将来の収益の総和に等しいというのが基本的な考え方になる。

これをファンダメンタル価格と言う。もちろん実際の金融商品の価格はファンダメンタル価格の通りに変動するわけではなく、そこから大きく乖離することはしばしばあるが、考え方のスタートラインとしては、金融資産は将来生み出すキャッシュフローによってその価値が決定するというのが基本となる。

この点、ビットコインをはじめとする暗号資産は、その仕組みとしては所有者に何の利益ももたらさない。満期に償還されるわけでもなく、配当が支払われるわけでもない。このような資産は、基本的には、ファンダメンタル価格を計算することはできない。すなわち、理論価格はゼロということになる。ビットコインの価格が大きく高騰していることに多くの金融人はとまどいながらも、「一時的なバブル現象であり、その価格は早晩また低くなる」と考えるのが



支配的であるように思う。

金融当局の人間や株式市場、為替市場のコメンテータが暗号資産について語ることはきわめて稀だが、何かの拍子に暗号資産について語らなければならないときには、苦笑を浮かべて突き放したようなコメントをすることが多い。ファンダメンタル価値の存在しない資産が一部の投資家によって高値で取引されていることに、金融のプロとして呆れた表情をすることが、1つのお作法になっているかのようである。

とはいえ、最近の暗号資産の急激な高騰や暗号資産の流通総額が200兆円を超える大きな存在になってきた結果、金融人の態度も変化しつつある。株式や債券の価格も、ファンダメンタル価格からの乖離が常態化する現象が観察される。人々がそこに何らかの価値を見出している以上、暗号資産の価格が高騰するメカニズムを分析していく必要があるだろう。

## 暗号資産の価格が高騰するメカニズム

金融商品と類似のものと考えれば理論価格が計算できない暗号資産が、一定の価格がついて人々の間で交換されているのは、暗号資産が金融商品とは異なる特徴を持つからである。暗号資産の取引の実態はすべてが明らかにされているわけではないが、いくつかの仮説を考えることは可能である。

最も基本的な仮説は、暗号資産が持っている匿名取引の特徴を利用した犯罪目的での利用価値があるということである。2013年のキプロス危機において国際送金が可能になったということがビットコインの相場を大きく引き上げたことは有名であるが、同じく2013年に米国で摘発されたシルクロード事件<sup>3)</sup>においても、ビットコインがさまざまな武器や麻薬の取引の決済手段として利用されていたことが知られている。現在でも、国際的な麻薬取引やマネーロンダリング事件の報道において、暗号資産が使用されたと報じられることは多い。ランサムウェ

アでビットコインが要求される事件も頻発している。暗号資産が犯罪者にとっての便利なツールになっていることは否定できない。こうした利用価値があるのであれば、プラスの価格が付くことも理解できる。

しかし、もし暗号資産の利用価値がそうした犯罪目的だけなのならば、暗号資産がここまで公のものとなり、多くの投資家に投資されているのも不思議である。暗号資産の犯罪利用を規制する動きは世界各国で強化されつつあり、犯罪者にとって利用しにくくするための努力が続けられている。そうした努力が有効であり、犯罪目的が唯一の利用目的であるならば、暗号資産の相場が高騰していることは矛盾する。

もう1つの仮説は、暗号資産には、犯罪行為以外にも、インターネット上で経済活動を行う際に有用な利用価値があり、新たなビジネスを生み出し、社会の効率化や高度化に寄与するというものである。新たなプロジェクトによって暗号資産の有用性が高まれば、暗号資産の価格の上昇を何某か正当化できるかもしれない。

とはいえ、これまでのところ、暗号資産が生み出す新たなビジネスについての事例は限られている。存在するプロジェクトも、暗号資産が高値で取引されることを出発点として、新たな暗号資産を次々に生み出すようなものが多い。ビットコインには発行上限額が存在し、マイニングで新規に生成されるビットコインは4年ごとに半分に減少するという希少性の源泉であったはずなのだが、ビットコインから派生した新たなコインやトークンの類が次から次へと生み出され、ビットコインと似たような値動きをする新たな暗号資産が増えているというのは、果たしてビットコインの理念と整合的なのだろうか。

また、そうしたプロジェクトは概して短命であり、試行錯誤の連続のように見える。もとより、新たな産業を生み出すイノベーションのためには、失敗はつきものだ。しかし、暗号資産関連のプロジェクトは、そもそも金融に近いビジネスであることもあつ



て、プロジェクトを通じて資金調達を行うことが可能である。結果として、多くの一般投資家を巻き込み、失敗すれば損失を与えることになる。通常の産業であれば金融機関を通じて規制を受けて行う資金調達を、規制を受けずに自ら実行できることはよいことなのだが、その分、投資家保護が十分ではないということになる。

結局のところ、取引されている暗号資産の根源的な価値らしきものを遡っていくと、それは暗号資産の取引による値上がり益の期待に帰着するという、自己回帰的な説明になってしまう。確かに暗号資産の相場は急速に上昇したけれど、とはいえ現在でも暗号資産に価値があるということについて納得できている人は少ないと思われる。

だとするとこの暗号資産に基づく新しい金融という考え方は砂上の楼閣であり、ベースとなる暗号資産の価値が本当に存在するのか、それらのものが人々によって維持され得るのかという点については疑義がある状態である。

暗号資産が大きく値上がりしたことによってあたかもその価値が永続するかのような感覚が出始めているけれど、健全な常識に基づく正確な理解と十分な警戒が必要ではないだろうか。

#### 参考文献

- 1) Nakamoto, S. : Bitcoin: A Peer-to-Peer Electronic Cash System.
- 2) 金融庁 : ICO (Initial Coin Offering) について～利用者及び事業者に対する注意喚起～ (2017.10.27).
- 3) Bearman, J : SILK ROAD: THE UNTOLD STORY (2015). <https://www.wired.com/2015/05/silk-road-untold-story/>

(2021年5月19日受付)  
(2021年7月29日note公開)

■岩下直行 iwashita.naoyuki.7e@kyoto-u.ac.jp

1984年、慶大経卒業、日銀入行。情報技術研究センター長、下関支店長、金融高度化センター長、FinTechセンター長を歴任。2017年、日銀を退職。京大教授に就任。金融庁参与および内閣府規制改革推進会議委員を兼務。

