寄稿論文

仮想通貨をめぐる現状と今後

京都大学公共政策大学院教授
岩　下　　直　行

《構　成》

Ⅰ　価格暴騰で一躍脚光を浴びた仮想通貨
Ⅱ　ブロックチェーン技術とは
Ⅲ　ビットコインのノードの実際
Ⅳ　マイニング作業の実際
Ⅴ　ビットコインが消費する電力
Ⅵ　ビットコインの黎明期：パソコンマニアによる実験
Ⅶ　ビットコイン価格の乱高下：キプロス危機による覚醒
Ⅷ　2017年の仮想通貨の大相場：ビットコインを上回るアルトコインの高騰
Ⅸ　2017年の相場高騰の原因：ＩＣＯ
Ⅹ　ＩＣＯの実態と今後の規制の在り方
Ⅺ　諸外国におけるＩＣＯへの規制
Ⅻ　2018 年入り後のコインチェック事件と相場調整

Ⅰ　価格暴騰で一躍脚光を浴びた仮想通貨

仮想通貨は、2017年に価格が高騰し、一躍脚光を浴びた。代表格であるビットコインの１通貨単位（１BTC）当りの価格でみると、2017年１月は1,000ドル/BTC程度で推移していたが、2017年12月には20,000ドル/BTCと20倍近い値上がりを見せた。ビットコインの価格が大きく上がる度に、テレビニュースに映像が流れたのも記憶に新しい。

この高騰は、金融のプロフェッショナルの予想を超えた現象であった。ファンダメンタルを重視するエコノミストは、資産の裏付けもなく、国家や企業の信用にも基づかない仮想通貨の本源的価値はゼロであり、価格はゼロ円に収束すると公言してきた。市場実勢を重視するプロのトレーダーも、仮想通貨は理論価格を算出できず、また取引業者の事故や破綻への備えがないことを嫌気して、投資を行わなかった。実際、主要国の金融機関や機関投資家のほとんどは、仮想通貨に投資していない。仮想通貨投資は専らアマチュアである個人投資家の手によって実施され、彼らだけが、2017年の大相場の利益を独占することになった。

人々から注目され、大きく値上がりしているのだから、ビットコインが通貨として商品の購入に便利に使われているか、というとそうではなく、ビットコインや他の仮想通貨が決済に利用された実績はほとんどない。BTCはドルや円に対して激しく変動している。法定通貨を基準に生活している消費者や販売者が決済手段として利用するのはリスクを伴い、不便でもある。仮想通貨はその名前に反して、価値尺度や交換手段、価値貯蔵手段といった「通貨としての機能」を果たしてはいないのだ。それでは、テレビや新聞で報道される「ビットコインが使えるお店」は、どんなからくりで存在するのだろうか。

「ビットコインが使えるお店」を仕掛けたのは、日本のビットコイン交換業者である。この業者が全ての取引リスクを引き受ける形でビットコイン決済の導入を働きかけ、先進的な小売店としてのイメージ向上を狙う企業と思惑が一致したのである。

こうした小売店店頭でビットコインを用いて資金決済を行う場合、店舗側が用意したスマホと顧客のスマホを用いて、ＱＲコードの読み取りを行うと、直ちに決済が完了する。しかし、実際にはビットコインが客から店へと移動するのではなく、ビットコイン交換業

者のデータベースが書き換わるだけだ。売上代金は、後日、ビットコイン交換業者から販売店に銀行口座への送金により支払われる。つまり、ビットコインで取引が行われているというよりも、店舗側の売上債権がビットコイン交換業者への債権につけ変えられることにより、円建てで決済が行われているに過ぎない。

このような取引を行うことによって、ビットコイン交換業者としては、「全国で決済に使える未来のお金」というイメージを広められる。小売店側としては、「業界初の未来の決済手法に対応した」という評価が得られ、メディアにも露出するので、広告宣伝効果が大きい。実際のところ、価格変動の大きいビットコインで実際に買い物を行う顧客は限られており、取引件数は微々たるものとのことだが、それでも、ビットコイン交換業者も小売店も、導入したこと（及びそれがメディアに取り上げられること）にメリットを感じているために、このような仕組みが維持されているのだ。

Ⅱ　ブロックチェーン技術とは

この仮想通貨ビットコインの基礎技術が、ブロックチェーン技術と呼ばれ、FinTech の中核技術として様々な解説がなされている。「ビットコインは、ブロックチェーン技術を仮想通貨に応用したもの」と説明されることも多い。しかし、実際の誕生の経緯は逆であり、まず、2008 年にビットコインが考案され、そこで用いられていた技術をより一般化した呼び名としてブロックチェーン技術という言葉が生まれた。そこでまず、最初に登場したビットコインの実現方法について解説しよう。

ビットコインは、サトシ・ナカモトを名乗る正体不明の人物が 2008 年に論文[1]を公表し、2009 年に最初のバージョンを開発した。それは、インターネット上で利用可能な電子現金を作ろうという実験であった。

ビットコインは個人間での送金にＰ２Ｐネットワークを利用することで、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取引においては、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。

こうした決済システムが機能するためには、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異なり、ビットコインは情報なので、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。その情報を再度使うの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、「センターを持たない」という理念に反し、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、二重使用をした者自身が検証者を兼ね、自らの不正な取引を「正しい」と検証してしまう恐れがある。

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して識別することにした。この特殊な計算によって連鎖する新しいブロックが生成される。こうした作業が「マイニング」と呼ばれ、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、

[1] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System"

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。そして、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。

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。

Ⅲ　ビットコインのノードの実際

具体的にビットコインのノードはどう構成されているのだろうか。bitnodes.earn.comというサイトでは、全世界でビットコインのノードがどのように分布しているかを随時更新している。それによれば、2018 年 10 月における全世界のノード数は 10,007 台であり、国別には米国、ドイツ、フランスの順に多く設置されている【図表１】。これらは同サイトから到達可能なノードのみを示したものであるが、現時点のネットワークの実態を概観する意味では有用な情報である。

日本のノード数は 246 台で、世界で 11 位である。ビットコインの取引金額の統計によれば、2016 年以降の日本のシェアはかなり高いが、それに比してノード数は少ない。これは、日本のビットコイン保有者が、自らノードを立てて取引を行うのではなく、専ら仮想通貨取扱業者を経由して購入していることを反映している。個人投資家が業者を通じてビットコインを購入した場合、その投資家は自らがノードを立てる訳でも、自らの取引をマイナーに承認してもらう訳でもない。その取引はブロックチェーンには書かれず（オフチェーン取引）、投資家は、取引所名義でブロックチェーン上に管理されたビットコインの一部を所有しているという情報が取引所に記録されるだけである。

【図表１】世界的なビットコイン・ノードの分布状況

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Oct 18 2018 12:27:03 GMT+0900 (日本標準時).

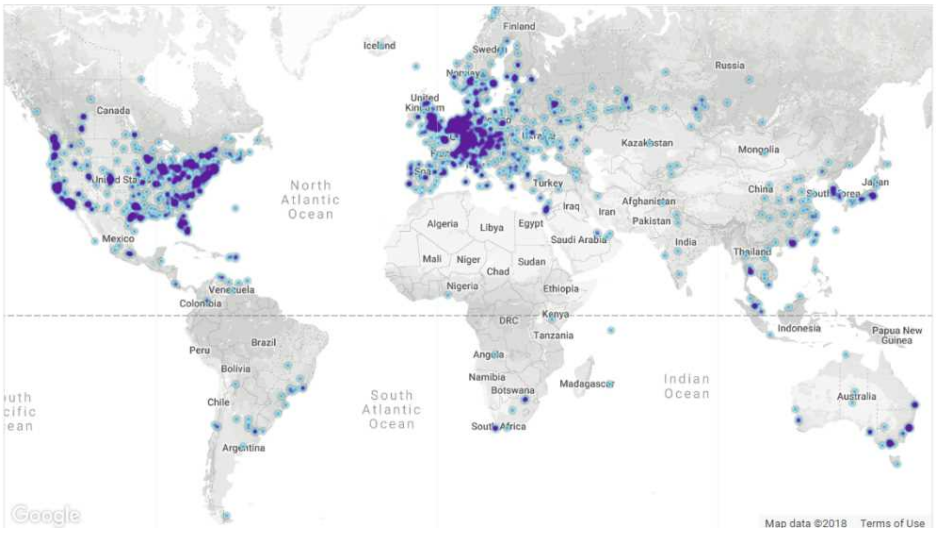
10007 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2375 (23.73%)
2	Germany	1933 (19.32%)
3	France	672 (6.72%)
4	China	672 (6.72%)
5	Netherlands	497 (4.97%)
6	n/a	458 (4.58%)
7	Canada	370 (3.70%)
8	United Kingdom	306 (3.06%)
9	Russian Federation	272 (2.72%)
10	Singapore	251 (2.51%)

More (99) »



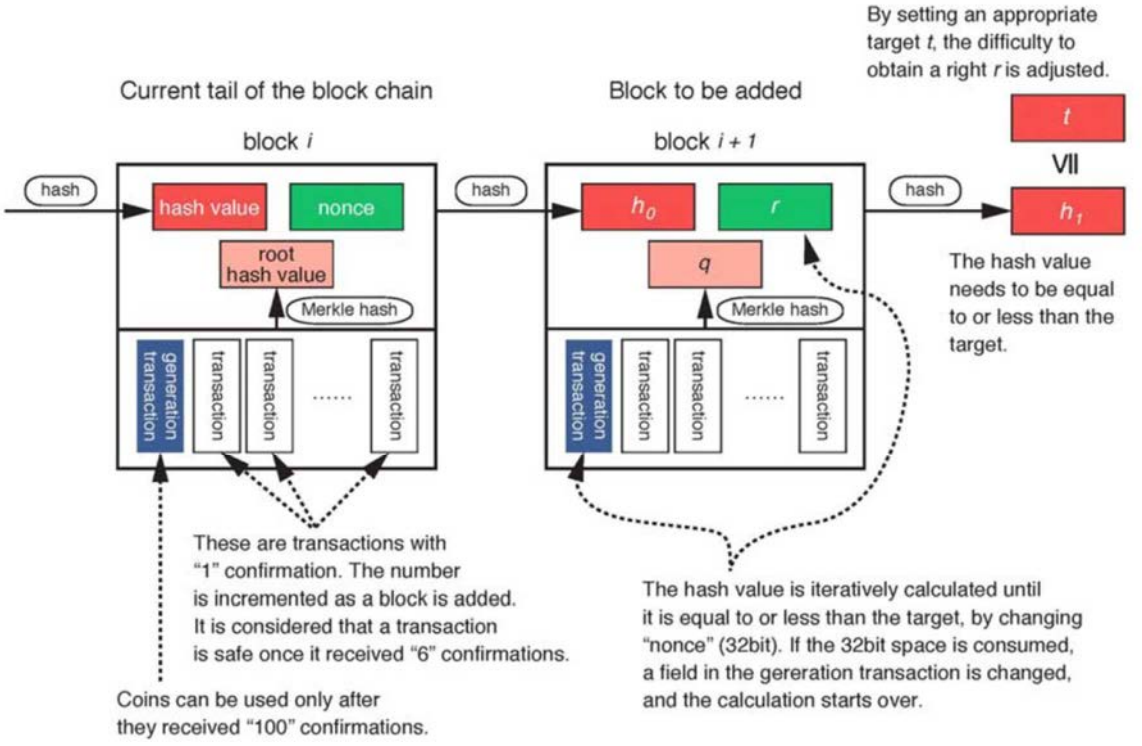
Ⅳ　マイニング作業の実際

ビットコインにおけるマイニング（採掘）とは、ハッシュ関数（データを固定長のハッシュ値に変換する関数）を使って時系列のデータをリンクさせ、（事実上）書き換えることが不可能なデータの連鎖を作り出す作業のこ

とである。ビットコインが何がしかの「価値」をやり取りする手段と位置付けられたのは、インターネットというオープンな環境に置かれながら、「データが改竄不可能」という特徴を持っていたからで、これが最大のメリットと考えられている。その技術を電子現金に使えばビットコインになるが、他の用途にも使えるのではないかということで、ブロックチェーン技術という言葉が使われるようになった。

ビットコインのデータのリンクの部分の作り方、つまり、マイナーによるマイニング作業は、以下のとおりである【図表２】。

【図表２】ビットコインにおけるブロック生成の模式図



まず、ビットコインの次のブロックを生成しようとするマイナーは、まだ承認されていないビットコインの取引を検証するところから始める。各取引に利用された電子署名が正当なものか、過去の取引履歴から計算して、取引後のビットコインの残高がマイナスになることがないかなど、ビットコインの取引環境を監視する役割を果たす。そして問題ないと判断された取引を組み合わせてルート・ハッシュ値を計算する。ここまでの作業負担はさして重くはない。

そして、前のブロックから得られたハッシュ値と、今回得られたルート・ハッシュ値、それに nonce と呼ばれる一種の乱数を組み合わせて、新しいハッシュ値を作る。このハッシュ値が、その時に決まっている条件（例えば、冒頭 20 ビットが０）を満たしていれば、それでマイニングは成功である。マイナーは、12.5 BTC のマイニング報酬（新規に発行されたビットコイン）を受け取ることができる。

しかし、実際にはそんなにうまくは進まない。生成したハッシュ値は、基本的に全ての

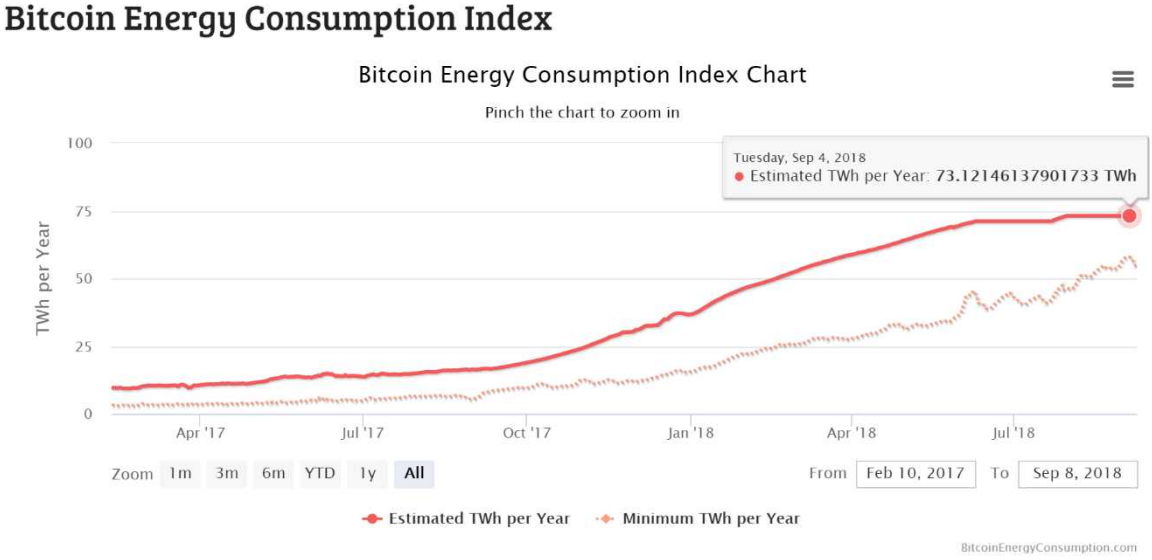
ビットがランダムに設定されるから、どのビットも０となる可能性は 1/2 と考えることができる。このため、$(1/2)^{20}$ の確率でしか、この条件は満たされないのだ。これは、約 0.0001%（1/1,048,576）の確率でしかない。そこで、マイナーは、nonce を少し変えてみる。するとハッシュ値は全く違ったものとなるが、それが条件を満たす確率も約 0.0001%である。マイナーが一人しかいない場合、この条件を満たすハッシュ値が見つかる確率が 50%になるためには、試行を約 72 万回行わなければならない。これが、膨大なハッシュ値の計算を行わなければならない所以である。このため、マイナーは、SHA-256 のハッシュ関数の計算のみに特化した特殊なハードウエア（ASIC: application specific integrated circuit、特定用途向け集積回路）を多数搭載したマイニングマシンをマイニングファームに設置して、マイニング報酬を求めて競争を繰り広げているのである。

Ⅴ　ビットコインが消費する電力

マイニングは専用のハードウエアを設置して適切にチューニングすれば、確率の問題で報酬を得ることができる。ただし、このマイニングマシンは膨大な電力を消費する。2017 年のビットコインの価格高騰の結果、消費電力は急激に増大した。現在マイニングに使用されている電力は、１年間換算で 73TWh（テラ・ワット・アワー）にのぼるという【図表３】。ここの数値は、オーストリア１国が１年間に使用する電力（約 72TWh）に匹敵する水準だ。

ビットコインの価格が高騰し、マイニングのための投資が活発になればなるほど、マイニングの難易度（ハッシュ値の何桁目までが０であるか）が上がって、消費電力が大きくなる傾向にある。条件に合うハッシュ値を探索するために費やされたエネルギーは、何か有用なものを生み出す訳ではなく、浪費されるだけだ。今後更にビットコインの価格が上昇するということは、この浪費が増大し、地球環境問題に発展することを意味する。これは、ビットコインの抱える深刻な問題のひとつである。

【図表３】ビットコインのマイニングに要する電力の推計値



（出所）bitcoinenergyconsumption.com

Ⅵ　ビットコインの黎明期：パソコンマニアによる実験

ここでビットコインの誕生から現在までの歴史を振り返ってみよう。2009 年１月９日、サトシ・ナカモトと名乗る人物が、ビットコイン v0.1 と名付けたソフトウェアを公開､配布して、実験を開始した。ビットコインは、当初２～３年間は、特に一般の人々から注目されることもなく、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。

ビットコインは、ドルや円といった法定通貨で価値を表示せずに、独自の通貨単位 BTC を利用している。発行主体が法定通貨と同じ価値で買い物等ができることを保証した電子マネーですら、利用者に信用され、受け入れられるには時間が掛かった。まして、独自の通貨価値を持つ仮想通貨は、買い物にも価値の貯蔵にも使いにくいので、人々から受け入れられることはなかった――ビットコインの出現までは。

マニアの間で交換や発掘が繰り返される中で、BTC の法定通貨との交換価値は徐々に上昇していく。当初はほぼ無価値であったが、2012 年には 20 ドル/BTC 程度の「相場」が成立するようになっていた。当時のビットコインは、インターネットの闇サイトでの麻薬や武器の取引に使われていたといわれる。米国における巨大闇サイト「Silk Road」の成立から、捜査当局による首謀者の逮捕までを描いたノンフィクション「The Rise and Fall of Silk Road」の中に、当時の状況が詳細に描写されている。同書では、「Silk Road はある意味では、インターネットを活性化させてきたリバタリアン的価値観の論理的帰結だった」と記述されているが､ＰＣ､インターネット、ビットコインと進化してきたＩＴの根底にあるリバタリアン的な発想が、巨大闇サイトの拡大を生み出したという点を指摘しておきたい。

Ⅶ　ビットコイン価格の乱高下：キプロス危機による覚醒

ビットコインがマニアのお遊びから、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 28 日のキプロス危機であった【図表４】。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徐々に上昇していく。

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 1,200 ドルにまで値上がりした。

【図表４】

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仮想通貨交換所、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 ドル近くに下落する。

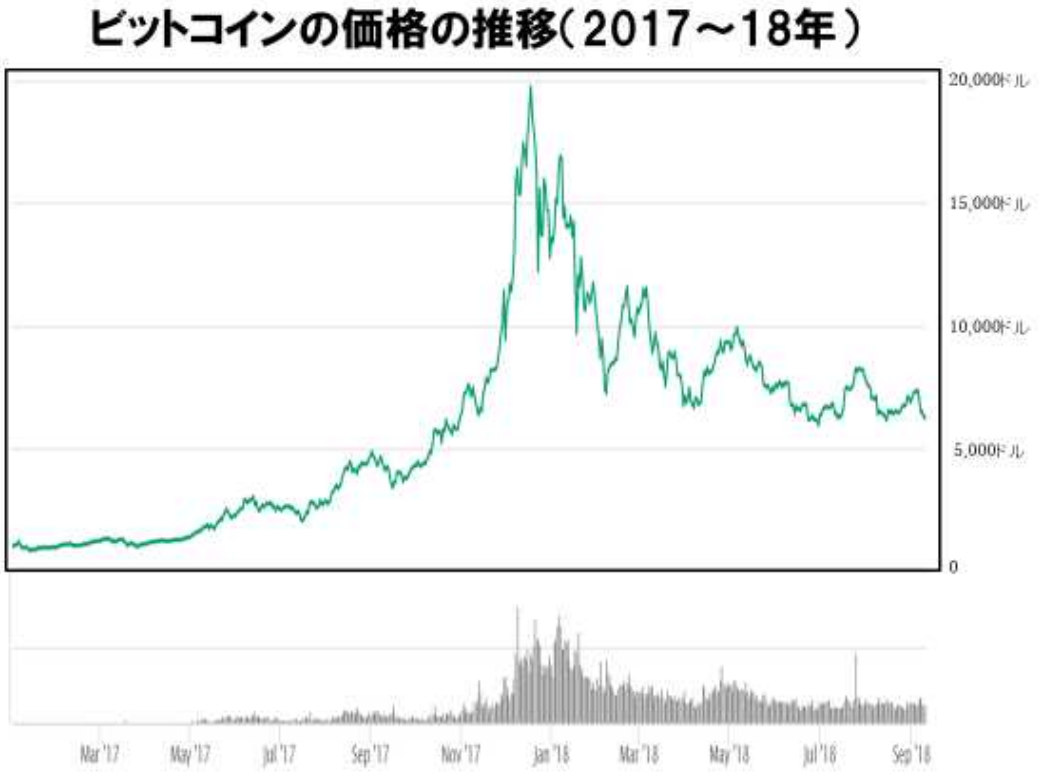
この状態がしばらく続いた後、2016 年になって相場は回復を見せ始める。その背景には、国際的な資金移動への利用が拡大したことや、「未来のお金」として注目され、個人が投機目的で購入する事例が増えたことなどが挙げられるが、何が正解かはよく分からない。

たとえ国家や企業の信用による裏付けがなくても、誰かが高値で買い取ってくれそうなものには値段が付くし、それは人々の期待に応じて変動する。とりわけ、この時期は世界的な金融緩和の時期であり、主要国の中央銀行は政策金利のターゲットをゼロ近傍としていた。こうした行き過ぎた金融緩和が、仮想通貨の相場を押し上げたことは事実であろう。

Ⅷ　2017 年の仮想通貨の大相場：ビットコインを上回るアルトコインの高騰

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【図表５】。相場が大台を超える都度、マスコミが大きく報道し、相場への注目は否応もなく高まっていった。

【図表５】

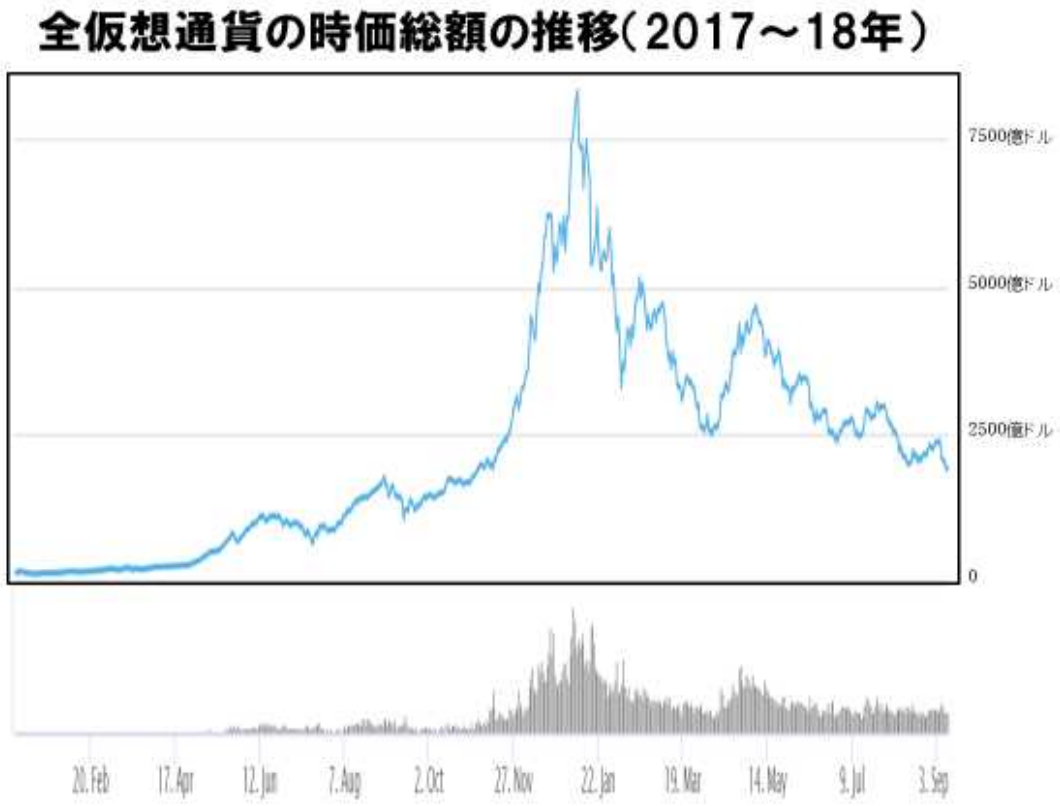


（出所）coinmarketcap.com

40

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。2017 年におけるビットコイン以外の仮想通貨の値上がりはより激しく、年間を通した仮想通貨全体の流通総額の上昇は、実に 50 倍近くに達し、日本円にして 2 兆円（177 億ドル）から 90 兆円（8,300 億ドル）への拡大である【図表６】。日本における現金通貨の発行残高が 100 兆円、個人保有の東証１部上場株式の時価総額もその程度だから、それに匹敵する規模にまで拡大したことになる。その後、2018 年に入ると、ビットコインもその他の仮想通貨も相場が急落する。流通総額は一時 30 兆円（2,500 億ドル）とピークの 1/3 以下にまで値下がりし、その後も乱高下を繰り返している。

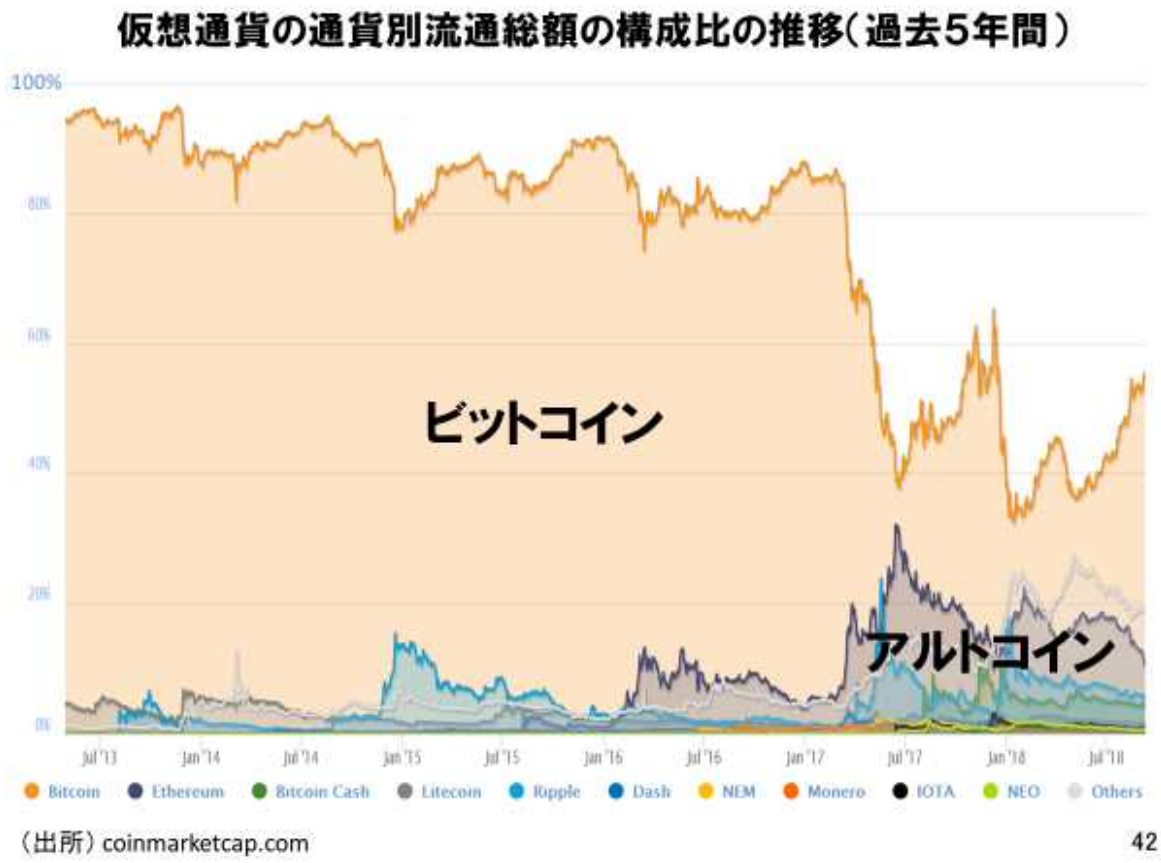
【図表６】



（出所）coinmarketcap.com　41

既に述べたように、2017 年には、ビットコインの相場は 20 倍になった。他方、全仮想通貨の流通総額は 50 倍になった。この結果、仮想通貨市場全体に占めるビットコインのシェアは、85%から 40%弱へと半減している【図表７】。その変化は、2017 年５月頃を起点に、きわめて短期間に生じている。過去には、ビットコインのシェアが 80%を下回ることはほとんどなかった。このため、2017 年の仮想通貨に起こったことを理解するためには、ビットコインだけではなくて、他の仮想通貨（アルトコイン）も含めて考える必要がある。

【図表７】



Ⅸ　2017 年の相場高騰の原因：ＩＣＯ

2017 年の大相場の原動力は、ＩＣＯ（Initial Coin Offering）であったと考えられる。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[2]」である。そのメカニズムについては、多少説明を要するだろう。

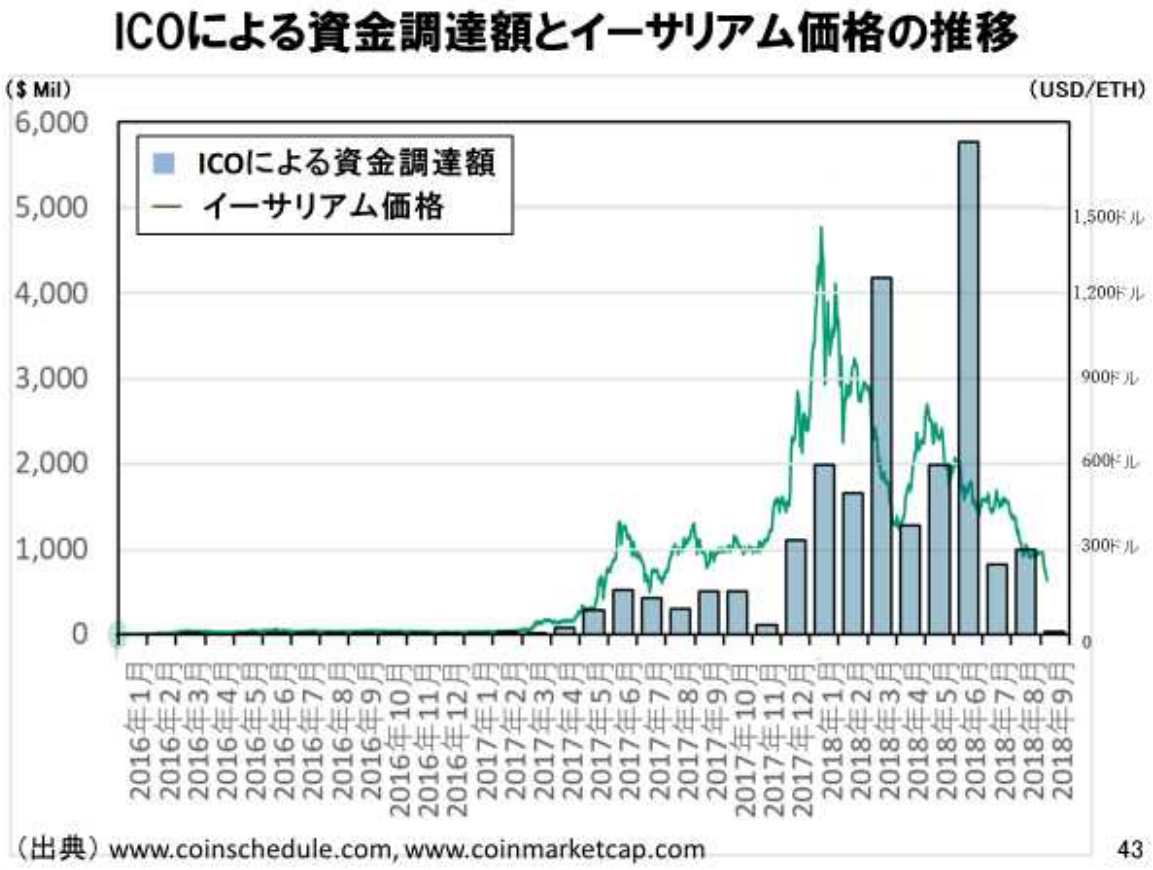
ＩＣＯの大半は、仮想通貨イーサリアムを基盤に利用し、ＥＲＣ－20 トークンと呼ばれる仮想通貨的なデジタル資産が発行される。この購入にはイーサリアムが必要になるので、ＩＣＯが増えると、イーサリアムの需要が増え、相場が上昇する。また、ＩＣＯトークンは払込金を償還するようなものではないのだが、イーサリアム建てで発行されるから、イーサリアムの相場が上昇すると、トークンのドル建て価格は上昇する。その結果、トークンの流通市場での価格が高騰し、それが更なるＩＣＯの活性化をもたらす。このような正のフィードバックが働いて、2017 年５月を起点にＩＣＯ発行額とイーサリアムの相場が急騰することとになったと考えられる【図表８】。

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（実際には、将来にも決済に使われることは難しいのだが）。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種類の仮想通貨が値上がりすると、それ以外の通貨も、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仮想通貨が、一斉に値上がりを始めたの

[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

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仮想通貨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仮想通貨に値上がりが伝播していく。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ものと考えられる。

【図表８】



そして、2017 年の仮想通貨の大相場の最後を飾ったのは、ＣＭＥとＣＢＯＥにおけるビットコイン先物の上場であった。先物が上場されれば、仮想通貨も正式な金融商品と認められ、金融機関や機関投資家の莫大な投資資金が市場に流入するかもしれない、そんな期待が、ビットコインの価格を僅か３週間で 10,000 ドルから 20,000 ドルに押し上げることになったのだ。

Ｘ　ＩＣＯの実態と今後の規制の在り方

ＩＣＯについて、もう少し具体的にみてみよう。ＩＣＯを計画するのは、実は企業とは限らない。仲間内で始めた新規事業の検討で事業計画を思いついた個人や、インターネットで募集した寄せ集めのグループのこともある。まず彼らが作成するのは、ホワイトペーパーと呼ばれる計画書だ。平均的には数十ページのこの文書は、「有価証券の募集・売出における目論見書のようなもの」と説明されることもあるが、実態はもっといいかげんなものだ。目論見書は投資家の投資判断の基準となる情報を提供するために発行され、一定の記載項目が定められ、虚偽記載があれば損害賠償責任を負う。これに対し、ホワイトペーパーは法的な裏付けもなく、記載内容も統一

されていない。ＩＣＯトークン発行後に書き換えられることも少なくない。

ＩＣＯで発行されるトークンもまた、有価証券とは異なる。株式のように配当を受ける権利や経営参加権を持つものでもなく、社債のように期日が来れば償還されるものでもない。ＩＣＯ発行体が手掛ける事業がうまくいった場合に、その事業で利用することのできる割引券のようなものが付いてくるだけである。これをユーティリティトークンと称する。この結果、ＩＣＯ発行体はほぼノーオブリゲーションで発行代り金を手にすることができる。

常識的に考えれば、資金調達を行おうとする際には、何らかの配当や償還を約した証券を発行した方がうまくいきそうである。しかし、ＩＣＯトークンが仮に配当や償還を約したものであったならば、それは各国の証券法上の有価証券と判断されるリスクがある。有価証券を一般大衆に発行するのであれば、証券法上の開示規制や各種行為規制の対象となる。ＩＣＯ発行体は、こうした規制を回避したいのだ。そこで、ユーティリティトークンとすることによって、いわば「無価証券」の形態をとり、規制を逃れるのだ。

不思議なのは、そんな無価値なトークンを買う人がいることだが、このＩＣＯトークンは大人気で、発行企業のウェブサイトに投資家が殺到してなかなか繋がらないという。投資家は何故このトークンを買うのであろうか。それは、流通市場で売却して売却益を稼ぎたいからだ。実際、2017 年にＩＣＯトークンを買い、年末まで保有した投資家は、平均で購入額の 3.2 倍の価格で売却できたという。

「ＩＣＯを発行市場で買って流通市場で売れば儲かる」という噂は瞬く間に仮想通貨投資家の間に広まり、ＩＣＯの大ブームをもたらし、それが先述のフィードバック効果で仮想通貨の高騰をもたらしたのである。

こうしたブームに乗って資金調達を行った発行体が、優れた製品・サービスの開発を行い、経済成長に寄与するのであれば、ＩＣＯにも意味はあるだろう。しかし、借入や株式発行ではなく、ユーティリティトークンによるノーオブリゲーションの資金調達を行った場合、その資金が有効に利用されるとは限らない。実際、ある調査によれば、ＩＣＯ発行体のほとんどが、何の製品も開発できていないともいわれる。

ベンチャー企業家は、ＶＣなどからの借入金を返済し、事業を成功させて富を得たいという夢があるからこそ必死で事業に取り組むのであって、ホワイトペーパーを書いただけで大金が手に入ってしまったら、苦労して事業を完遂する気にならなくても不思議ではない。ＩＣＯへの投資家も、流通市場でトークンを高く転売できればいいのであって、事業が最終的に成功するかどうかにあまり関心はない。その結果、ホワイトペーパーの内容は曖昧かつ粗雑になりがちであり、中には文書として完成していないものも含まれていたが、それでもＩＣＯトークンの販売に影響はなかった。さすがに、2017 年末以降、トークンが売れずに不調に終わるＩＣＯも出てきているが、「ノーオブリゲーションで資金を手にしたい」と願う発行体は引きも切らない状態が続いている。

ＩＣＯの仕組みは、いわば壮大なババ抜きゲームである。発行体と発行市場の投資家の双方が大儲けするものの、流通市場で高値掴みした投資家は、最終的に無価値なトークンを抱えることになる。発行体の事業が仮に成功したとしても、その果実がトークン所有者に還元される訳ではないから、マーケットの過熱が収まれば、トークンが無価値になることはほぼ確実だ。その意味で、きわめて非倫理的な仕組みなのである。

Ⅺ　諸外国におけるＩＣＯへの規制

このように様々な問題をはらむＩＣＯに対して、各国の規制当局が規制に乗り出している。

米国では、ＳＥＣがＩＣＯの一部は米国証券法上の有価証券の公開売出に該当するとの見解を表明した。明らかに詐欺と思われるＩＣＯの募集を行った者を告発するといった対応も進めている。また、米国証券法上の「私募」の規定を適用し、適格投資家に限定した募集を行うことを認めたものもある。ただし、本来は認められないはずの一般公衆への転売が行われているとの情報もあり、規制が適切に機能しているかは今後の確認を要するだろう。このように、米国はＩＣＯ全体を証券法制で規制する方向にある。

一方、中国は、2017 年９月にＩＣＯを禁止した【図表９】。中国の金融規制機関が連名で出した声明文によれば、「ＩＣＯが経済と金融の秩序を破壊した」と厳しく指摘している。中国には当時、65 ものＩＣＯプラットフォームがあり、毎週 10 件ものＩＣＯの募集があったという。相場が過熱し、ビットコインとは何であるかすら知らない高齢者たちが老後資金を投入し始めるに至って、当局が規制に乗り出したのではないかという現場の声も報じられている。

そして、日本も 2017 年 10 月に金融庁が注意喚起を公表している【図表 10】。

【図表９】

【図表 10】

日本の金融庁もICOに対する注意喚起を公表

ＩＣＯ（Initial Coin Offering）について
～利用者及び事業者に対する注意喚起～

29.10.27 金融庁

1．ＩＣＯとは

○　一般に、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す。トークンセールと呼ばれることもあります。

2．利用者の方へ（ＩＣＯのリスクについて）

○　ＩＣＯで発行されるトークンを購入することには、次のような高いリスクがあります。

✓ 価格下落の可能性
トークンは、価格が急落したり、突然無価値になってしまう可能性があります。

✓ 詐欺の可能性
一般に、ＩＣＯでは、ホワイトペーパー（注）が作成されます。しかし、ホワイトペーパーに掲げたプロジェクトが実施されなかったり、約束されていた商品やサービスが実際には提供されないリスクがあります。また、ＩＣＯに便乗した詐欺の事例も報道されています。

（注）ＩＣＯにより調達した資金の使い道（実施するプロジェクトの内容等）やトークンの販売方法などをまとめた文書をいいます。

○　トークンを購入するに当たっては、このようなリスクがあることや、プロジェクトの内容などをしっかり理解した上で、自己責任で取引を行う必要があります。

Ⅻ　2018 年入り後のコインチェック事件と相場調整

2018 年入り後、仮想通貨の市況は調整局面に入った。ビットコインの価格も、全仮想通貨の流通総額が、僅か１か月程度でピーク比の 1/3 に下落している。

相場下落の一つの原因は、仮想通貨法の登録が未了のみなし業者であったコインチェック社が、時価 580 億円相当の仮想通貨ＮＥＭを不正に流出させる事件を起こしたことだ。何者かが同社の管理する電子署名用の秘密鍵を不正に利用し、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る手続きをしてしまった。顧客から預かった資産が盗まれてしまったのである。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。

今回の事件はなぜ起こったのだろうか。顧客の大事な資産である仮想通貨を預かる立場として、コインチェック社の体制は不十分であった。コインチェック社は、26 万人の顧客から預かったＮＥＭを一つの大きな財布に入れていた。その財布は、常時インターネットと接続され、そこから資産の出し入れが可能な状態にあった。その財布から仮想通貨を移転する手続きは、たった一つの暗号鍵によって守られていたにすぎない。この暗号鍵の管理が杜撰であったのだろう、鍵が不正に利用されて、ＮＥＭが送金されてしまったのである【図表 11】。

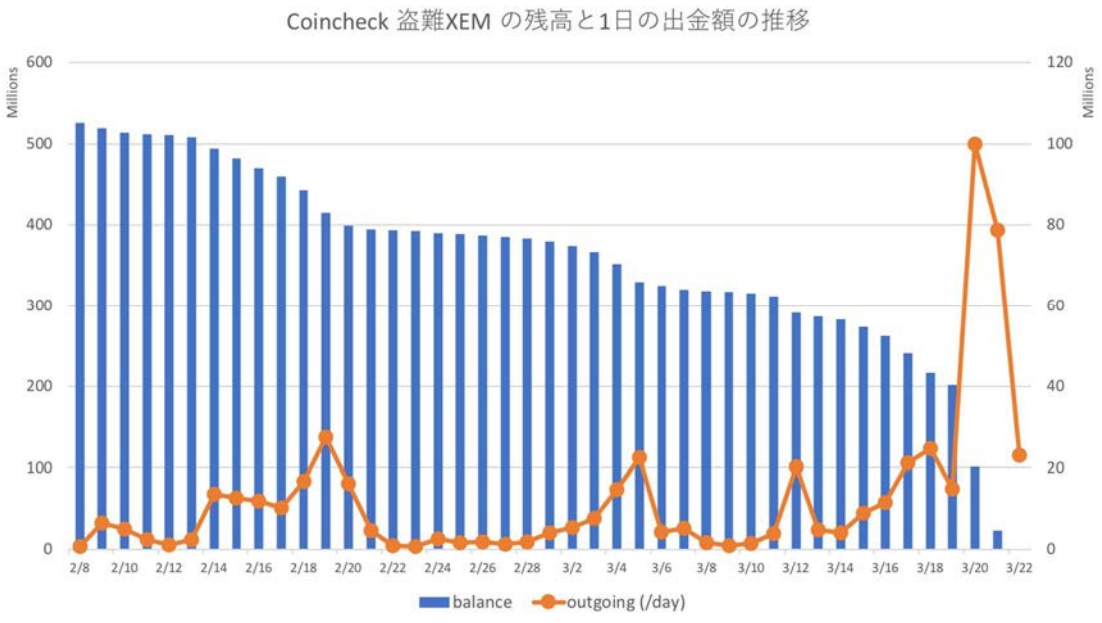
【図表 11】コインチェック事件におけるＮＥＭの動き

時刻	金額(XEM)	送金元	送金先
2018/1/26 8:26	800,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 4:33	1,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:35	1,500,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:29	92,250,000	NC4C6PSUW5	NA6JSWNE24Y
2018/1/26 3:28	100,000,000	NC4C6PSUW5	NDDZVE32WB
2018/1/26 3:18	100,000,000	NC4C6PSUW5	NB4OJJCLTZW
2018/1/26 3:14	100,000,000	NC4C6PSUW5	NDZZJBH6JZP
2018/1/26 3:02	750,000	NC4C6PSUW5	NBKLOYXFJVF
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWFIZ
2018/1/26 2:58	50,000,000	NC4C6PSUW5	NA7SZ75KF6Z
2018/1/26 2:57	30,000,000	NC4C6PSUW5	NCTWFIOOVIT
2018/1/26 0:21	3,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:10	20,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:09	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:08	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:07	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:06	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:04	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:02	10	NC3BI3DNMR2	NC4C6PSUW5

【図表 11】において、黄色で示した「NC3...」というアドレスは、コインチェック社の名義のアドレスである。このアドレスに、顧客から預かったＮＥＭ580 億円分が保管されていた。他方、赤色で示した「NC4...」というアドレスは、犯人が用意したものである。１月 26 日の午前０時２分に最初の 10 XEM が送金され、その後、20 分足らずの間に、523,000,000 XEM が送金された。犯人は、このアドレスから更に別の複数のアドレスに送金している。更に、午前３時、４時、８時にも、NC3 から NC4 への不正な送金を行っている。

もちろん、最も糾弾されるべきなのは、この不正送金を実行した犯人だ。正体不明のこの犯人は、自らが管理することになった 580 億円分のＮＥＭを、少しずつ闇サイトを通じて他の通貨と交換し、資金洗浄を進め、まんまと逃げおおせてしまった【図表 12】。

【図表 12】盗まれたＮＥＭはどうなったか？



日本は、他国に先駆けて仮想通貨交換業者を規制する法律を施行し、業者の登録制度を運用してきた。しかし、それは資金洗浄やテロ資金調達を防止することが主眼であった。現在の仮想通貨法は、交換業者が多額の顧客資産を預かる存在であることを意識した、十分な利用者保護の仕組みを備えていない。業界も、信託や保険といった仕組みを活用して、自主的に被害を限定する取り組みを進めるべきである。また、セキュリティ対策の基準を制定し、ディスクロージャーを徹底することにより、利用者の不安の払拭に努める必要がある。今回のような事件が再び起きないように、常に対策を最新のものとする工夫も必要である。

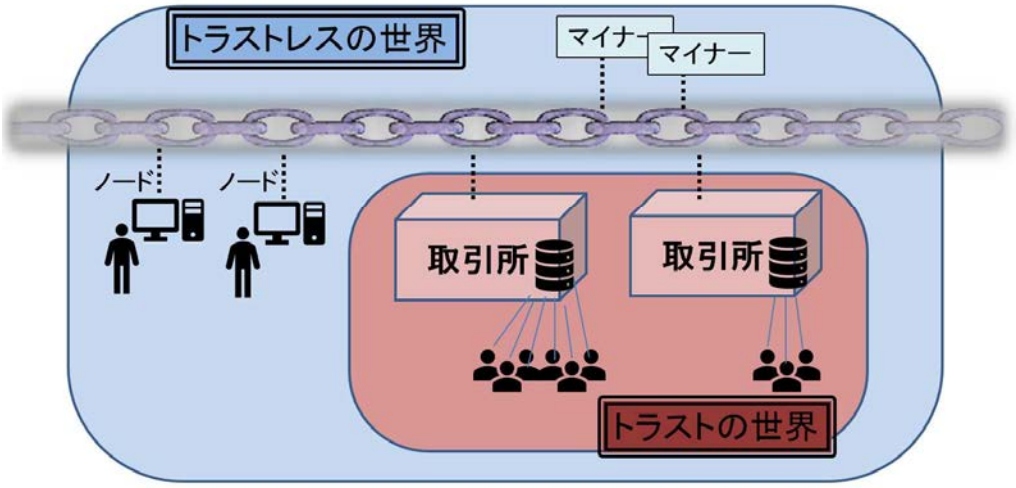
今回の事件で誰もが不思議に思うのは、不正送金されたＮＥＭが犯人のアドレスに送金されていることは確認できるのに、それを取り戻すことができないという点である。これがもし、銀行預金であったなら、盗まれた大金がどこかの預金口座にあることが分かった時点で、当局によって差し押さえられ、最終的には盗まれた人に返還されると期待できたであろう。

ビットコインが注目され始めた当初から、その背景に特殊な思想があることが注目されてきた。それは、信頼できる中央機関を決して置かないというポリシーで、「トラストレス」と呼ばれる考え方のことだ。ビットコインは、こうした特徴を持つからこそ、法律や政治体制の違いによる国境の壁を易々と越えて、国際的な利用が可能になったと考えられる。

これに対し、信頼できる中央機関を置く従来の仕組みを「トラスト」の世界と呼ぶ。我々は、政府、中央銀行、裁判所といった信頼できる中央機関の存在を前提に構成された世界に住んでいるから、トラストレスの世界は、きわめて特殊な、危なっかしいものに見える。とはいえ、ビットコインの存在は認知され、トラストとトラストレスの両者が併存する状況が続いてきた。

例えば、ビットコインのノードとして直接接続している geek な利用者は、トラストレスの世界で生きている。しかし、自らがノードに接続することのできない素人の利用者は、取引所にビットコインを預け、取引所に依存してビットコイン取引を行っている。この場合、そうした利用者にとって、取引所こそが「信頼できる第三者」であり、そこにトラストの構造が存在する【図表 13】。

【図表 13】「トラストレスの中のトラスト」構造の問題



今回流出したＮＥＭは、トラストレスの世界で盗まれ、資金洗浄された。信頼できる中央機関はなく、国家権力を含め、何者も情報を恣意的に書き換えることはできないという建前だ。今回のＮＥＭの問題をみれば、それが両刃の剣であることが分かる。

仮想通貨という異質な存在を、国家が適切に制御すること、つまり、その利点を生かし、欠点を補うことができるだろうか。この新たな課題に向き合うためには、国際的な規制対応も含め、関係者が知恵を絞っていくことが必要となるだろう。