

続々：成るか、ビットコインによる通貨革命？

酒井 寿紀 (Sakai Toshinori) 酒井 IT ビジネス研究所

前々号と前号でビットコインの行政面から見た問題などを取り上げた。本号では、ビットコイン自身が抱えるより本質的な問題を何点か取り上げよう。

通貨供給量の制約が大

まず第 1 の問題は、通貨としての供給量に大きな制約があることだ。

一般的に、通貨の供給量は経済活動の伸展に伴って増加する。例えば、日銀券発行高は、1980 年初めには 15.7 兆円だったが、2010 年初めには 77.8 兆円と、30 年で約 5 倍になっている。

しかし、ビットコインの発行高は、生まれてから 4 年経った 2012 年末に 1,050 万ビットコインになり、その後新規発行高は 4 年ごとに半減するので、総発行高は永久に 2,100 万ビットコインを超えない。

長期的に世界の経済活動が拡大し、それに伴って一般の通貨の発行高も増大すると、ビットコインの位置付けは低下する一方だ。

無制限に通貨を発行すれば、通貨の価値が下がってインフレを招くので、それを避けるためにビットコインは発行高に厳しい制限を設けている。しかし、その結果ビットコインの希少価値化が進んで激しい値上がりを招けば、初期の投資家は喜ぶかもしれないが、決済手段としての役目を十分に果たせなくなる恐れがある。

資源・電力の無駄遣い

ビットコインは、全取引をインターネット上の台帳で公開し、この台帳に最近の取引をまとめて追記してくれる人を募って、この人たちに報奨金としてビットコインを与える。しかし、報奨金目当ての応募者が殺到しすぎては困るので、難しい計算問題を速く解いた人だけに追記を認める。

この報奨金のビットコインを採掘するために、全世界で大量にコンピュータと電力が使われている。少ない費用で競争に勝つには、安価・低電力で高速なコンピュータを使う方が有利なため、汎用のパソコンの他、高速の演算回路を付加した装置やビットコインの採掘専用に開発された LSI を装備した装置も使われている。

これらの装置の費用や電気料金を正確に把握することは困難だが、全世界で膨大な量になると言われている。しかし、採掘者に課された仕事の成果は、「賽の河原の石積み」と同じで何の役にも立たない。

改良版が次々と登場

ビットコインのこれらの問題を解決しようと、改良版が次々と現れている。

その 1 例は 2011 年 10 月に現れたライトコイン(Litecoin)である。これは、最近の取引をまとめて台帳に登録する間隔を、ビットコインの 10 分から 2.5 分に縮めることによって、取引が確認されるまでの時間を 1/4 に短縮するとともに、供給量を 4 倍に増やした。よって、総供給量は

8,400 万ライトコインになる。

また、採掘に使う計算問題を、演算の並列化による高速化が困難なものに変え、特殊な装置の有効性を減らした。

もう 1 つは、2012 年 8 月に現れたピアコイン(Peercoin)である。これは、ビットコインと同じように、問題を解いた採掘者に通貨を供給するとともに、ピアコインの所有者に対して毎年所有量の約 1% を新規に供給する。したがって、ピアコインの供給量には上限がなく、永久に増加を続ける。

そして、供給量の増えすぎを防ぐため、すべての取引に対して定額(現在は 0.01 ピアコイン)の手数料を課し、徴収した手数料を市場から抹消することによって供給量の適正化を図っている。

また、2013 年 7 月にプライムコイン(Primecoin)が現れた。ビットコインは資源と電力の浪費が大きいので、プライムコインは採掘者に課す仕事を「ある条件を満たす素数の列の発見」にし、数学的に意味があるとともに、暗号技術にも使えるものにした。プライムコインという名前は「素数(Prime Number)」から付けられたものだ。

そして、このプライムコインの供給量には上限がなく、採掘者に課す問題の難易度の調整によって変更できる。

現在このような仮想通貨が 100 種類以上現れていて、仮想通貨が広く一般化する兆しが見える。そして、その大半は上例のようにビットコインをベースにした

ものなので、ビットコインの技術が将来の仮想通貨の基盤になるものと思われる。しかし、ビットコインにも弱点があり、各種の改良版が現れているため、ビットコイン自身が将来の主役になるかどうかは不明だ。

ただ、本年 4 月現在、仮想通貨の時価総額の上位 100 種中、ビットコインが全体の 90% を占め、他は合計して 10% に過ぎない。そのため、当面はビットコインを中心にして各種の仮想通貨が共存する時代が続くと思われる。

金融政策が不可能に

将来仮想通貨が現在の通貨の役割りを一部代替えるようになると、現在の銀行やクレジットカード会社の仕事が減ることになる。そのため、これらの企業は既得権益を手放すまいと必死になって抵抗すると思われる。

そして、ある程度以上この代替えが進むと、中央銀行や財政当局は金融政策の手段を失うことになる。また、金融政策の効力を信奉する、いわゆるマネタリストの経済学者は自説の基盤を揺るがされることになる。そのため、これらの人たちは仮想通貨の普及に対する大きな抵抗勢力になるだろう。

したがって、仮想通貨は、当面は決済手段などを代替える補助的な通貨として、現在の通貨と共存して使われることになるのではなかろうか？