(C)日本経済新聞社 無断複製転載を禁じます。

ポイント
- ビットコインの採掘は無意味な計算作業
- 自発的な採掘によってシステム維持可能
- マクロ的には金本位制と同様の特性もつ

エコノミクス・トレンド

小林慶一郎 慶大教授

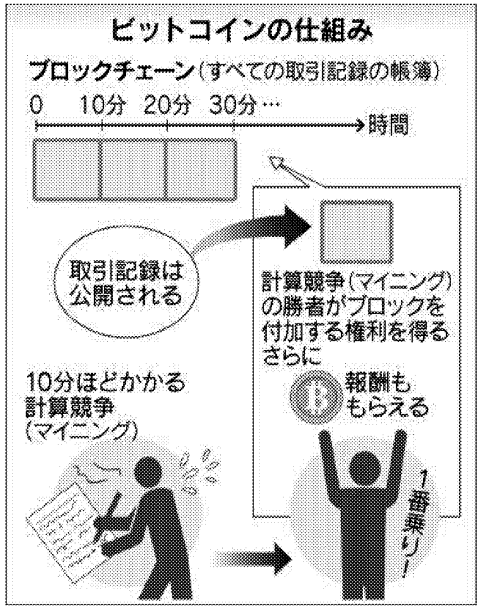
仮想通貨の技術的可能性

市場経済、構造変化も
貨幣による公共財供給へ

分権型の仮想通貨「ビットコイン」は、貨幣の本質的な性質を斬新かつ巧妙な方法で実現したものだといえる。ビットコインの実体はネット上に存在する過去から現在までのすべての取引記録の帳簿（ブロックチェーンと呼ばれる）である。この帳簿には、全世界のビットコインに関するすべての取引が記録されている。各参加者は、このブロックチェーンを自分のコンピューターやスマートフォン（スマホ）で同期し、共有する。

●●● ●●●

一般に、「支払い」が成立するための本質的要請とは、「取引の不可逆性」と「安全性（二重払いなどの不正防止）」が通貨システムで確保されることである。取引の不可逆性とは、あとで支払いの事実が（データ改ざんやしらばっくれなどで）否認できないことである。紙幣や硬貨による支払いなら、貨幣を物理的に受け渡した事実によって、取引の不可逆性は成立する。二重支払いの問題も、紙幣や硬貨なら、Aさんに支払った貨幣をBさんにも支払うのは物理的に不可能だ。しかし、ネット上ではデータのコピーが容易なので、不可逆性や安全性の確保が重要になる。



不可逆性と安全性を実現するためにビットコインが採用している中核的アイデアが、マイニング（採掘）によるブロックチェーンの延伸である。ビットコイン経済では、約10分ごとに、過去10分間の全世界すべてのビットコイン取引を記録した取引記録（ブロック）をブロックチェーンに付け加えることで、ブロックチェーンを延伸していく。

ビットコインの取引は即時に公開され、付加すべきブロックの内容はビットコイン参加者のコンピューターで共有されているが、それをブロックチェーンに付加できるのは、ある「計算課題」をコンピューターで解いた参加者に限られる。この計算課題はサイコロを振るのと同じような作業で、まったく無意味な計算だが、解くのに10分程度かかるよう設計されている。この計算の答えをプルーフ・オブ・ワーク（時間をかけて作業をしたことの証明）という。

計算課題の正解にもっとも速く到達した勝者が、最新のブロックをブロックチェーンに付加することができ、さらに報酬としてビットコインを新しく創造し自分のものにできる。この「計算課題」を解く競争に参加することを、金鉱の採掘になぞらえてマイニングという。この設計によって、ビットコイン参加者の分権的かつ自発的行動の結果として「取引の不可逆性」と「安全性」が確保される。

取引記録を改ざんするには、改ざんしたい記録の時点から現時点までのブロックチェーンを不正に改ざんし、本物だと他の参加者に信じ込ませなければならない。ところが不正なブロックチェーンを作るには、改ざんしたい記録の時点から現時点までのすべての「計算課題」を解きなおす必要がある。取引記録を改ざんすると「計算課題」が変化する仕組みになっているからだ。1つの計算には10分程度の時間がかかるので、不正なブロックチェーンを作成する作業は、本物のブロックチェーンの延伸スピードに追いつけない。よって不正なブロックチェーンは作成できない。

参加者はこのことを知っているので「取引記録の改ざんは不可能だ」と確信できる。また、計算能力の高いコンピューターの所有者は、報酬目的で自発的にマイニングに参加する。不正なブロックチェーンをつくるより、マイニングで報酬を得る方が利益を得られるからである。ビットコインのシステムを破壊する不正よりも、システムを守る作業をする方が利益を得られるのだ。つまり、参加者の利己的な利潤追求によって「不可逆性」と「安全性」が確保される設計なので、政府などの管理者がなくても、ビットコインのシステムは自律的に維持され存続していく。

以上の記述は、野口悠紀雄著「仮想通貨革命」（ダイヤモンド社）、岡田仁志・高橋郁夫・山崎重一郎著「仮想通貨 技術・法律・制度」（東洋経済新報社）を参考にした。

●●● ●●●

ビットコインの巧妙な設計は、貨幣が持つ「外部経済効果」を内部化する仕組みだ、と理解することができる。

ビットコインに限らず、一般の支払いシステムにおいて、「取引の不可逆性」や「安全性」の確保とは、システム参加者みんなにとっては利益だが、個々の参加者（特に支払者）は、そのためのコスト負担をしたくない。放っておくと、参加者みんながフリーライダー（ただ乗り）になり、「取引の不可逆性」や「安全性」は維持できなくなる。「取引の不可逆性」や「安全性」は、それ自体は市場で取引できない外部経済効果であり、分権的なシステムでは、供給が過少になってシステムは崩壊する。従来はこの外部経済効果を確保するために、2つの方法が使われてきた。

第一は、有体物の貨幣（紙切れ、金塊など）の受け渡しによって支払う方法である。取引の不可逆性や安全性は、物体の持つ物理的性質によって容易に確保される。貨幣として使われる物体は、本来の使用価値よりも高い価値を持って流通する。その差は流動性プレミアムといってもよいが、取引の不可逆性や安全性を確保するコストだと解釈できる。

第二の方法は、信用力のある管理者（銀行）が不可逆性や安全性を保証する貨幣（すなわち銀行預金）による支払いである。不可逆性や安全性を確保するためのコストは、預金者から銀行への手数料として支払われる。

これら2つの方法に加え、ビットコインは貨幣システムの第三の方法を提示したという意味で画期的なのである。つまり、システムの参加者たちがマイニングという利潤追求活動を自発的にすると、結果的に不可逆性や安全性が確保されるようにシステムが設計されている。取引の不可逆性や安全性を確保するためのコストは、マイニング作業（無意味な計算による時間と電力の消費）で支払われる。

●●● ●●●

ビットコインのメカニズムは画期的だが、技術的な条件（採掘のコストなど）で貨幣供給量が決まるので、マクロ的には金本位制と同じような特性を持つと推測される。今後、ビットコインが普及したとしても、現存の主要通貨や金銀と競合する貨幣が一つ増えるだけで、マクロ経済運営に大きな影響はないかもしれない。しかし、仮想通貨は様々な新種が提案されている。今後、市場経済のあり方が変わる可能性もある。たとえば、マイニングを「意味のある計算」にすることである。

ビットコインのマイニングは無意味な計算だが、この計算課題を「温暖化防止に関連する（公共財的な）意味のある計算作業」にできれば、仮想通貨による経済取引の増大が地球温暖化の解決に役立つことになる。あるいは、マイニングの計算課題をゲノム解析に関連付けられれば、仮想通貨の普及が医学の進歩に役立つ。マイニングのための計算が、公共財を供給する作業にもなるわけだ。

ネット上の仮想通貨に限らず、「貨幣システムをうまく設計することによって公共財の私的供給を増やす」ことができれば、市場経済の姿は大きく変わる。ビットコインはそのような技術的可能性を開いてくれたのかもしれない。

4人の筆者が交代で執筆、原則、月1回掲載します。