2014.02.20 (No.8, 2014)

Newsletter

Institute for International Monetary Affairs
公益財団法人 国際通貨研究所

ビットコインの仕組みと課題

公益財団法人 国際通貨研究所
経済調査部長 兼 開発経済調査部長
佐久間 浩司
koji_sakuma@iima.or.jp

ビットコインは、使用の拡大は限定的と思われるが、通貨や金融の観点から非常に興味深い試みである。今後どう進化するかで経済への効果や影響は変わってくるだろうが、少なくとも現段階での特性を見る限り、一国のマクロ経済や金融システムの安定的な発展を阻害する要因になるとは思われない。

1. ビットコインの基礎知識

ビットコインについての最低限の知識は、現段階でのビットコインの公式に近いサイトであるbitcoin.orgに比較的分かりやすく説明があり、以下、若干の個人的解釈も交えて解説したい[1]。

(1)ビットコインとは

ビットコインとは、デジタル通貨の一つであり、またその通貨を媒体とする決済メカニズムである。世界で最初に明確にこのアイデアが提示されたのは、Satoshi Nakamotoという名前の人物が 2009 年に発表した論文「Bitcoin：A Peer-to-Peer Electronic Cash System」においてであり、以後、その論文に示された理論をベースに、システム発展に自発的に貢献するエンジニア群によって運営されている決済システムである。

[1] http://bitcoin.org/en/faq

（2）通貨発行や運営に関与する人・組織について

“デジタル通貨”とか“仮想通貨”というように「通貨」と呼ばれるので、発行母体やその責任や権限などはどうなっているのかというのが、多くの者が最初に抱く疑問だろうが、ビットコインはネットワーク型の組織で運営されており、ピラミッド型の指揮・責任の系統はない。また誰がそのネットワーク組織のメンバーかという正式な認証手続きも明確ではない。従って、事業目的などの公式文書もないし、それらを責任もって掲載するインターネット上の公式サイトもない。

2014 年 2 月現在、当事者的な視点に立ち、バランスよくかつ責任ある書き方でビットコインについて説明が記載されているのは冒頭述べた Bitcoin.org というサイトである。当サイトは、ビットコインのプロジェクト初期の中心メンバーで作成され、中でも中心的なメンバー6 名の名前とコンタクト先も明記され、ビットコインに関する疑問などについても受け付けている。但し、Satoshi Nakamoto 自身 2010 年末ごろにはプロジェクトにあまり関与しなくなったように、これらの 6 名や Bitcoin.org のサイトも自然に影が薄れる可能性はある。

この他に運営に関与する企業や個人が掲載されているサイトに Bitcoin Foundation のサイト Bitcoinfoundation.org がある。ここには、Foundation のメンバーとして、プラチナメンバー1 社、ゴールドメンバー2 社、シルバーメンバー63 社、また個人の永久会員約 400 名、年会員約 500 名など、プロジェクトに関与する法人・個人の名前が掲げられている。プラチナメンバーはビットコインが使えるオンライン店舗の bitcoinstore（米国カリフォルニア州）、ゴールドメンバーはビットコイン最大の取引所 Mt Gox（東京都渋谷区）、ネット金融企業者（米国デラウェア州）の名前がある。

（3）ビットコインを使うには

ビットコインを使うには所定のサイトに行き Wallet と呼ばれる入出金のための口座をオンライン上に開設する必要がある。口座開設には、パスポートや運転免許証などの身分証明書が求められ、少なくとも日本語のインターネットサイトを見る限り、匿名で口座開設はできない。ビットコインの取引は、オンライン上の ID を示すだけでできるが、Wallet 情報まで遡及すれば支払人や受取人を特定できる。

ビットコインの入手方法は二通りある。一つは財サービスの対価としてビットコイン建ての支払いを受け付ける、あるいは先述の Mt Gox のようなネット上の取引所で他の通貨と交換することである。もう一つは、Mining と呼ばれるビットコインの仕組みを維持するための貢献を通じ 1 作業当たり 25bit の報酬を得る方法だ。

ビットコインの取引所の取引量のシェア

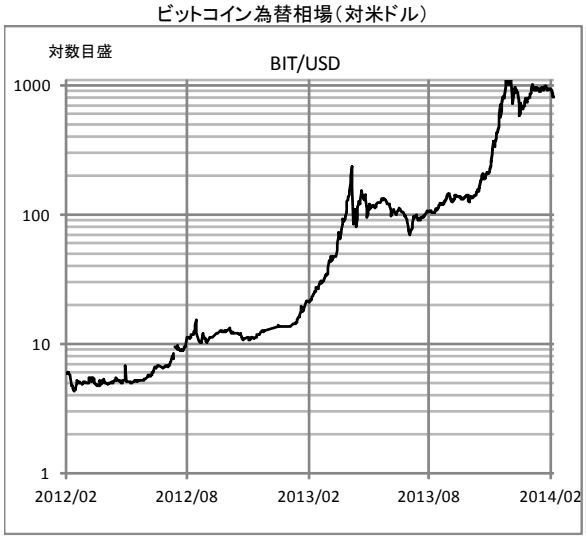
取引所名	取引シェア (%)
Mt.Gox	87.842
BTC-E	4.155
BitStamp	2.208
BitFloor	2.086
CampBx	1.723
CryptoXchange	0.808
BTCex	0.625
Intersango	0.489
BTC Tree	0.021
Vircurex	0.014
BitMarket	0.011
Bitcoin-24	0.008
Bitme	0.006
ICBIT	0.005
Total	100.000

(Source)Mt.Gox, as of August 2012

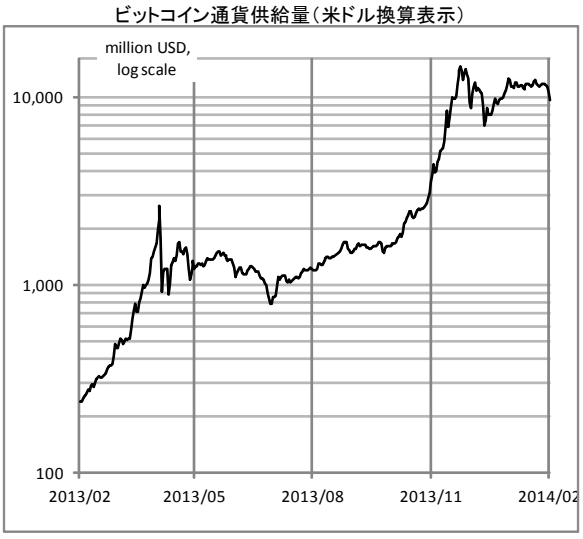
(4)ビットコインの流通状況

現在、ビットコインの為替相場は 1bit=693 ドルであり、マネーストックの総量は 12,364,850bit であるから、米ドル建てにすると、85 億ドルほどである（すべて 2014 年 2 月 7 日 17 時現在で、ビットコインの市場情報サイト bitcoinx.com による）。これは、他の金融ストック統計との比較では、2013 年 9 月末の国際決済銀行（BIS）に報告義務のある銀行（BIS 報告銀行）の全世界向け国際債権残高 19 兆 7600 億ドルの 0.04%、2012 年 12 月末の全世界の銀行資産残高 116 兆 9560 億ドルの 0.007%であり小さそうに思えるが、例えば香港における人民元建て預金残高は、2009 年ごろは今のビットコイン流通量くらいであった（現在の香港の人民元建て預金はその頃の 16 倍の 1378 億ドル）。小規模とはいえ、ある程度の存在感を示している。

支払手段としての現状は、2013 年 11 月現在、全世界でビットコインが使用可能な店舗は、オンラインではなく物理的に存在するという意味で 1700 店ほど、ネット上で 35,000 店と報告されている。日本では、物理的に存在するベースで 15 ある。決済件数は、全世界で 1 分当たり約 46 件と、VISA カードの 200,000 件の 4300 分の 1 であり、話題になっている割には、ビットコインの使用は広まっていない。



（Source)Blockchain.info



（Source)Blockchain.info

（5）ビットコインの信認維持の仕組み

①Mining

自分が受け取ったビットコインの真性（偽物でないという保証）は、Miningというシステムで作り出される。ビットコインはシステム的に 0.00000001 の補助単位まで細分化が可能とされるが、最小単位 1 単位ごとに所有者履歴が記録される。これは他の通貨にはないユニークなシステムだ。他の通貨や金（ゴールド）も、誰の財産かは記録されているが、お札や金塊そのものに所有者履歴が書き込まれるわけではない。Miningとは、所有者が移るたびに行われる電子媒体上の履歴更新作業のことをいう。履歴更新には書き込みパスワードの解読が必要で、この数学的な作業負荷こそがビットコインの信認維持の中心的メカニズムとなっている[2]。

ビットコインの取引情報は、オンライン上ですべてのビットコイン・ユーザーに公表され、それを閲覧したユーザーが自発的に取引記録をビットコインの台帳に書き込む[3]。この履歴更新には 25bitの報酬が付与される。またこの報酬とは別に、ビットコインの支払いを受けた者が履歴更新者に対して手数料を払ってもよいことになっている。こうした報酬+手数料というインセンティブのため、取引情報を閲覧した者の間でMiningは

[2] 通貨の所有者が電子的に記録されるという点は、手形や売掛債権に電子的に所有者情報が書き込まれる電子債権と似ている。違いは、期日のあるなしという現金と手形・売掛債権の一般的な違いの他に、システムの中心的な機関の存在がある。電子債権には、国から認可を受けた電子債権記録機関が存在し、そこで、個々の債権に書き込まれた所有者記録が管理されることでシステム全体の信認が維持されているのに対し、ビットコインは、こうした管理責任の所在が特定できる中心機関がない。

[3] 物理的にどこか 1 カ所に中心的なデータベースがあるのかはどうか不明だが、「台帳」的なものをイメージする方が分かりやすいので、本レポートでは便宜的にこのように説明している。

競争的に起こり、最初に暗号解読に成功したものに 25+αbitが支払われる。

取引記録が台帳に記帳されるということは、そのビットコインに正式に新しい所有者が記録されたことを意味する。このプロセスを認証（Verification）というが、認証されて初めて、ビットコインを受け取った者は、それを別取引の支払いに使える。認証が課されることによってビットコイン 1 単位 1 単位の真性が成り立っている。また、システム上、常にこの Mining 作業に 10 分程度の時間がかかるように設計されている。このシステムは、Mining を受けながら相手のコンピューターの能力を測り、どんなに計算力のあるコンピューターでもだいたい 10 分の負荷がかかるような暗号解読の難易度を調整できる。

②偽造防止の仕組み

ビットコインという通貨の信認の拠り所は、(a)Mining 作業に非常に高度な暗号解読の計算力が要求されることと、(b)Mining 作業の機会が誰にも開かれているため常時多数の者が報酬目当てに解読に取りかかっている、という二つの特徴によって偽造が極めて難しい点にある。

ビットコイン 1 単位は、生まれてから所有者変遷履歴がチェーンのように繋がって書き込まれているが、今、ある偽造者が最新の受取人を自分に仕向けるように偽の履歴を書き込もうとしたとする。つまり偽の履歴のチェーンを繋げようとしたとする。この時、偽の履歴を正統なものとしてネットワーク全体に認知させるためには、当該ビットコインが生まれて以降の全履歴を書き換える必要があり、そのために要する時間は、例えば所有者の購入履歴が 5 回分あれば、過去のMining 5 つ分と同じだけの時間、すなわち 10 分×5＝50 分の時間がかかる。これに対し、圧倒的多数の善意のMinerたちが真性な履歴をつけようと競い合っている。こちらの方は、システム的に直近の履歴を追加するだけの作業であり、約 10 分で完了する。偽造者は、とても善意の不特定多数には勝てないことになる。これが、ビットコインの偽造防止の基本的なメカニズムだ[4]。

（6）ビットコインのシニョレッジ（通貨発行益）

Mining に挑むものは、相当程度の数学・情報工学の専門知識を持っていなければならず、また、かなりの資金をコンピューターに投じなければならない。この Mining とい

[4] オープン参加型のシステムで、善意の参加者が悪意の参加者を駆逐するメカニズムを利用したものに Wikipedia がある。これは、偽情報を書き込んでも、圧倒的に多数の善意の参加者によって正しい（と多数派が信じる）情報に書き換えられてしまうため、結果としては、正しい情報が生き残る確率が高いというメカニズムだ。ビットコインの偽造防止は、このメカニズムに似ている。

う能力も資金も必要な貢献に対し与えられる 25bit が通貨発行のシニョレッジである。通常は国家が法律、決済システム、関連官庁などのハードインフラ、ソフトインフラを整備し、通貨のユーザーの便宜を図るために汗をかき、その膨大な負荷と引き換えに通貨発行の利益、すなわちシニョレッジを享受する。

国際通貨の世界で、米国が基軸通貨発行国としてシニョレッジをただで享受しているという見方があるが、米国は、ドルを基軸とする国際金融秩序の維持のために莫大なコストを負担しており、この批判は正しくない。中国が人民元国際化において、貿易決済における元建て促進には熱心だが、基軸通貨を目指しているわけではないのも、この負担を考えてのことと思われる。

ビットコインの場合は、この技術負荷がシニョレッジの対価となる。このシニョレッジ 25bit は、ビットコインの通貨供給量が増えるにつれて逓減する仕組みになっている。ビットコインが流通し始めた 2010 年の 50bit からスタートし、だいたい 4 年ごとのペースで報酬額は半減する。すなわち、2014 年には 25bit、2017 年には 12.5bit、2021 年 6.25bit、2025 年 3.125bit となり、ビットコインの流通通貨量増加スピードも徐々にゼロに近づき、最終流通残高は 2100 万 bit となる仕組みになっている。

2. ビットコインの評価と課題

(1)ビットコインへの過度な警戒は不要

基本的にビットコインは、一国あるいは一経済地域において主要な通貨になることはないという前提に立てば、今指摘されているような懸念のほとんどは杞憂で終わる可能性が高い。資本取引が自由な国においては、利便性を感じる者の間で使われればよい。

①投機に関する懸念

投機によってビットコインの価値の乱高下は、今までもあったしこれからも続こうが、これは株、証券化商品、金、不動産など、投資の対象となるあらゆるものと同じであり、購入した者は価値の乱高下で損を被るかもしれないが、関与しない者まで含めて経済全体に害が広がるとは思えない。

②ポンジスキームではないかという懸念

ポンジスキーム（ネズミ講のように最後に受け取ってしまったものが損をする仕組み）との批判はあるが、これはどんな通貨も、ひとたび信認がなくなれば最後に受け取ってしまったものが損をするのは同じことであり、ビットコインだけの懸念材料ではな

い。

③匿名性とマネーロンダリング（資金洗浄）に関する懸念

ビットコインの持つ匿名性によってマネーロンダリングに利用されるという懸念があるが、先述の通り Wallet を開設する際には本人確認がなされるため、政府が必要な法的措置をとれば匿名性の問題は解決できると考えられる。

④デフレ・スパイラルを招くという懸念

通貨供給量が機械的に最大 2100 万 bit と決められているため、将来ビットコイン需要が伸びればデフレが進行するという懸念があるが、確かに需要が伸びれば財サービスに対しビットコイン 1 単位の価値は上がっていくだろう。しかし、どこの国でもビットコインが唯一の通貨であるわけではなく、決済システムの中であくまで限定的な範囲で使われる限り、ビットコインを使用できる店の方で価格を書き換えれば済む話である。消費全体の先延ばしや借入への躊躇などのマクロ経済活動のブレーキにはならない。

（2）金融取引通貨としての限界

こうした諸々の懸念が杞憂であろうという理由は、ビットコインが信用創造につながる通貨になる可能性の低さにある。もともと、銀行を介さない決済手段というのがビットコインを作った意図の一つであるため銀行が扱う可能性は低いのだが、仮に何らかの形で銀行がビットコイン建ての預金を受け入れるようになったとしても、それが貸出に回る可能性は低い。

銀行は、いつ引き出されるか分からないお金を不特定多数の預金者から集め、期間のリスクを負って貸出を実施する。もし、期間のミスマッチが起こりそうになったら、インターバンク市場で借り入れ、さらにそこでも資金調達が難しい場合には、その通貨を発行する中央銀行から借り入れる。こうした二重のバックストップに守られて貸出業務を行っている。特に中央銀行の存在は、地場通貨に関しては絶対安心なバックストップである。

銀行は、この流動性のセーフティネットのないビットコインでは、積極的な貸出ができない。銀行貸出が起きないということは、信用創造が起こらないため、マネーストックの量はマネタリーベースの量以上には膨らまない[5]。

[5] ビットコインを使っての貸し借りは起こりうる。今、オンラインの世界でビットコインの売買情報や取引所で為替レートが提示されているのと同様に、貸したい人、借りたい人が、金利や期間などの条件を提示し合い、二者間で合意して所有者が移転すればいいだけである。しかし、これは企業間金融と同じで、マネーの保有者が貸与という形で A 社から B 社に移り、満期になればそれが戻ってくるだけであって、銀行を介さないため信用創造にはつながらない。マネーストックの量はいつまでたってもマネタリーベース

また、中央銀行が市中銀行に与える流動性のセーフティネットは、カスケード式（段階的）に市中銀行から一般の企業や個人に対しても当座貸越などの形で供与される。ビットコインには、この銀行システムを介して提供される流動性のセーフティネットがないのである。

こうしたマネタリーベース以上に残高が増えないという量的限界や流動性セーフティネットの欠如という限界のため、健全な通貨システムが機能している国であればビットコインがその国の決済において主導的な地位を持つことは考えがたい。また信用創造に使われる可能性が低いということは、ビットコインの価値が乱高下しても、その混乱が金融システムを介して大きな余波を生み出す可能性も低い。

（3）やがて Mining の速度が遅くなる可能性

ビットコインの将来の課題として、現段階で想定されるのは、信認の要である Mining という行為の起こる速度が、やがて遅くなって、使用者が利便性を感じなくなる可能性があることだ。

現在 Mining1 回当たりに Miner が得る利益は、25bit の Mining 報酬と、ビットコイン取引の受け手側からの任意の手数料である。手数料の金額は、小売業者がビットコイン建てで支払いを受けるメリットを考えると、クレジットカード決済の手数料 3%程度よりは低いと言われている。報酬の 25bit は、約 4 年毎に 12.5、6.25、3.125 と半減していくことになっており、やがてはゼロに近くなる。そうなると Miner たちの利益は手数料だけになり、結局、今よりは手数料水準を引き上げないと Mining が行われなくなることが十分考えられる。手数料水準が既存のクレジットカードなどの 3%のレベルに近づけば近づくほど、ビットコインでの支払いを受けるメリットはなくなる。この Mining のインセンティブの低下をどのように解決するのかが大きな課題と思われる。

＜参考文献＞

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, 2009

ECB: Virtual Currency Schemes, October 2012

経済産業省：電子記録債権制度への期待について　2014 年 2 月

の量と変わらない。

Address: 3-2, Nihombashi Hongokucho 1-chome, Chuo-ku, Tokyo 103-0021, Japan
Telephone: 81-3-3245-6934, Facsimile: 81-3-3231-5422
〒103-0021　東京都中央区日本橋本石町 1-3-2
電話：03-3245-6934（代）ファックス：03-3231-5422
e-mail: admin@iima.or.jp
URL: http://www.iima.or.jp