|  |  |  |
| --- | --- | --- |
| **時事エッセイ** | **シカゴ連邦** | **2013年12月** |
|  | **準備銀行** | **317号** |

シカゴ連邦準備銀行ニュースレター

**ビットコイン：初心者用ガイド**

*著者：François R. Velde、シニアエコノミスト*

# ビットコインは2009年に運用が開始されたデジタル通貨であり、近年大きな注目を集めています。本記事では、通貨の仕組みを解説してその特徴についての考察を加えます。

ビットコインは実に見事に構築されたデジタル通貨です。しかし、既存の通貨と競合したり、置き換えることは可能でしょうか？

今回のシカゴ連邦準備銀行ニュースレターでは、ビットコインと呼ばれるデジタル通貨について解説します。現在流通しているビットコインの総量は約1180万であり、実際の硬貨と異なって、小数点以下8桁まで分割できます。ビットコインはさまざまなオンライン両替サービスを通じて他の通貨へ交換できます。本記事が書かれた時点で、過去6ヶ月の平均ビットコイン価格は100ドルを少し上回る程度で推移しています。つまり、ビットコインの総額は10億ドルであり、それに対して米ドルの流通総額は1兆2000億ドルです。毎分平均してビットコイン取引が30回行われています（VISA取引回数は毎分平均20万回です）。ビットコインの平均取引額は16ビットコイン、つまり、約2000ドルです（平均VISA取引額は80ドル程度です）。ゆえに、ビットコインは比較的小さな現象と言え、着実に成長しています。ビットコインの価値は2013年初頭から現在までの間に10倍に膨れ上がりました。（注１）

**デジタル通貨とは一体何でしょう？**

金銭とは交換媒体です。価値のあるモノやサービスとの引き換え用として承認され、それ自体ではなくほかのモノやサービスと後々交換するために存在します。数千年にわたって、この媒体は希少価値のあるモノという形態をとってきました。自然から産出されるもの（希少金属）や人工的に作り出されるもの（独占的に発行される引換券）などです。しかし、実体を持たない場合もあります。売り手と買い手の間で、ある個人や

物体に対して強制力を持つ債権をやりとりする場合などが該当します。今日のアメリカにおいては、基礎通貨は貨幣（国会により承認を受け、米国造幣局が発行する引換券）と紙幣（連邦準備金制度の債権が流通していたのが以前の状態でしたが、今では紙の引換券そのもの）という実体を伴っています。また、連邦準備金制度の帳簿に載っている預金取扱機関の債権、という体裁をとった電子形式の準備金でもあります。

ビットコインは実体のあるモノや通貨に対する債権ではありません。それ自体が通貨であることを目的としており、実体をコンピューターファイルで置き換えただけです。実体のあるモノが交換される時、持ち主が既に所有しているものが受け手に渡されるのはほぼ間違いありません。（交換されるものが偽物でないかどうかが、金銭の場合は常に問題となりますが、解決する方法はいくらでもあります）。デジタルファイルは簡単に作成、複製ができます。通貨としての信憑性を確立するにはどうすればよいのでしょう？解決方法として、基本的には再帰法が選択されています。私が本物のビットコインファイルを確実に所有していると仮定します。私が取引を通じてビットコインの所有権を譲り渡した事実は、ビットコインプロトコルを通じて、全取引記録のデータベースに追加されることで認証されます。これで、受け手に所有権が渡ったことが認証されました。

取引の正当性を認証する簡単な手法は、

全取引の記録を保持する当局に一任することです。中世の商人は支払の際に取引額を記帳し、現代の銀行は連邦準備委員会の台帳に取引記録を記載することで、行ってきました。しかし、ビットコインは取引記録を一括して扱う管理者を持ちません。ビットコインはデジタル通貨の生成量を管理し、偽造を防ぐ一石二鳥の手法を

地中から掘り出すのが困難であり、アンが金貨を偽造していない「証明」になります。しかし、それはあくまでも、ボブが簡単に金の含有量を確認する方法を知っている場合にのみ機能します。ビットコインも、次の要領で採掘者たちの「採掘証明」を要求します：ブロックチェーンに正式に追記するためには、複雑な数式を解かなければなりません。これには非常に手間がかかります（パソコンの

そして、採掘者の貢献が認められます。解答を最初に見つけた採掘者は、他の採掘者に配信して検証を依頼します。一旦検証されると（つまり、他のノードの大部分から受け入れられると）、新ブロックはチェーンに追加されます。この幸運な採掘者は、努力が報われて *N* 個の新ビットコインを手にします。

ビットコインのプロトコルには、長期にわたって *N* と α の値を管理する部分もあります。困難さの指標である α は隔週ごとに調整され、新規ブロックが

# ビットコインはデジタル通貨における2つの課題－生成量の管理と偽造防止－を一度に解決できます。

一時間に6回の割合で追加されるようにしています。従って、より多くの採掘者がネットワークに参加したり、パソコンの処理能力が向上すると、それに伴い難度も上昇します。報酬額の指標である

採用しています。認証は実行が難しく、

それを行える人間には条件付きでビットコインを新規発行する権利が与えられます。

**発行／認証手順**

ここから、より技術的で詳しいやり方でプロセスの解説を行っていきます。次の状況を頭に思い描いてください：アンはビットコイン（後に本質を解き明かしますが、要するに0と1が並んだ数列です）を所有しています。ビットコインは「財布」（暗号化を施されたコンピューターファイル）に入れられ、パソコンや携帯デバイスにインストールされたアプリケーションで管理できます。彼女はビットコインをボブに渡します。ボブも、アプリケーション経由で管理された「財布」を所持しています。両者のアプリケーションは取引を行います。（取引を安全に行うために、公開鍵と秘密鍵が用いられます。例えて言えば、相手が品物に鍵を掛けられるように、南京錠を送りつけるようなものです。ただし、南京錠の鍵は、自分が所持したままです。）この時点では、アプリケーション側では、アンとボブが取引の提案を行っている、とインターネットに広がる大規模なノード群に情報を配信する段階にとどまっています。（より正確に記すと、お互いの公開鍵を通じて特定された、アンとボブの財布間の取引です。）毎10分毎に、「採掘者」と呼ばれる各ノードが最近配信された取引提案を集め、「ブロックチェーン」、またはビットコイン取引の全記録を収めた台帳に追記しようとします。

ブロックチェーンの偽造を防止する手法の要として、追記には非常に困難な作業が伴うようになっています。アンとボブが金貨を交換している、と過程します。金貨に含まれる金は

ハードウェア能力、電力消費、

かかる時間の点で）。数式を解くのは困難ですが、解答を検証するのは簡単です。因数分解（注2）を行うのは困難ですが、因数分解の解答が正解であるかどうかを確認するのは簡単であるのと同じです。

さらに、数式は任意に選ばれたり、どんなものでもよいとされているわけではありません。取引自体の検証にも利用されているからです。

最後に、もう一つ技術的な解説を行います。ハッシュ関数は様々な長さのテキストや数字を固定長の数列に変換します。例えば、ある言葉の最初の文字を取り出すと（あるいは、ある数の桁を加算し、結果の桁をさらに加算して、一桁になるまでそれを続けると）、どんな言葉や数字も1の長さを持つハッシュ値にマッピングされます。採掘者が解答する課題は、概して次のようなものです：ブロックチェーンを *x*、追記が提案されたブロックを *y* 、追記される数字を *n* とします。

1. 目的は、最終的に得られるハッシュ関数 *f* (*x*,*y*,*n*) が予め設定された値 α より小さくなるような *n* を見つけることです。ハッシュ関数は決定性ですが、あまりにも複雑なため結果はランダムに見えます。ゆえに、*n* を推定するのはほぼ不可能であり、唯一の信頼できる手法は、多くの異なる *n* の値を試し、条件が満足されるまで続ける他にありません（パソコンの処理能力を大量に必要とします）。さらに、 α の値が小さいほど、条件を満たすのは難しくなります。しかし、解答である (*x*,*y*,*n*) の正当性を検証するのは簡単に行えます。解答の *n* を得る過程の一部として、ブロック *y* 内で取引が行われたビットコインがブロックチェーン *x* でまだ使われていないことを検証する必要があります。

各採掘者は、ブロック *y* 内に特殊なタイプの取引を一つ埋め込むことができるようにコードが設計されています。その結果として、新規ビットコインが *N* 個発行されます。

*N* は初期設定では50であり、210,000ブロックごとに半減します（つまり、毎時6ブロックの速度で4年毎です）。つまり、存在しうるビットコインの総数は2 × 50 × 210,000 = 2100万に限りなく近づきこそすれ、絶対に超えないことになります。さらに、必要な時間はコンピューターの処理能力やビットコインネットワークの大きさとは無関係です。時間が経つにつれ、採掘は割が合わなくなっていきますが、代わりに採掘者には他の報酬が与えられるようになります：ユーザーは、新規ブロック内に取引を埋め込み、ブロックチェーンに追加する作業に対して報酬を払うことができます。この報酬は、ブロックを追加した採掘者に与えられます。

つまり、ビットコインはデジタル通貨を発行する上の課題を、実に見事に解決しているわけです。課題とは、発行量の調整、偽造と二重使用の防止、安全な移動の保証などを、中央当局に頼らずに行うことです。結局、この新しい通貨とは一体何なのでしょう？認証済みの取引一覧、と呼べます。通貨単位の発行に始まって、現在の持ち主に至るまでがすべて記載されています。受け手全員が過去取引を検証でき、新規取引を認証できる手段を持っているため、通貨の交換が可能となっています。また、所有権の拠り所はノード群の合意に基づいています（注3）。

**ビットコインは信用通貨です**

金貨や金に変換可能な紙幣といった商品通貨と比較して、信用通貨はそれ自体に価値を持ちません。価値は、政府が発行する不換紙幣や

誰かが受け取るはずだという信念から得られます。それゆえ、信用通貨は脆さを内包しています。政府の指示は無視されたり、疑われる可能性があり、価値があるはずだという信念からのみ価値を得ている通貨は、結局のところ価値を全く持たない場合もあります。（例えば、誰も支払に受け取らないだろう、と私が判断すれば、私だって受け取ることはしません。）

「採掘」という用語を使用しているゆえに、ビットコインや信用通貨ではない、と思われることがあります。ビットコインを毎日1つずつ生成する難しさは、現時点では3,000ドル程度かかるハードウェアを用いて、毎日1ドル程度の電力消費がかかる程度です。ハードウェアが5年間で減価償却されるとすると、ビットコインを1つ生成するコストは約

2.50どるとなります。しかし、一旦生成されると、金貨と異なりビットコインは交換する以外に価値がありません。

**ビットコインの通貨としての有効性**

ビットコインは既存の通貨（特に、現金の形態）と競合したり、あるいは置き換えたりすることができるのでしょうか？私が持っているドル札は同時に複数の場所に存在することはできません。私の所有権は確固としており、すぐに交換を完了することもできます。ビットコインは数多くの優れた特徴を持ち、現金と同じ特性を持てるようにしていますが、弊害もあります。主な

大きな脆弱性ともなっています。ビットコインが二重使用されていないかどうか、ネットワーク経由で認証が必要になります。最低10分間かかります（小額取引に関しては確認作業が不要な場合もあります）。さらに、「歯抜け」状態が発生する場合もあります。ネットワークのある場所で新ブロックが1つ承認されるのと同時に別の場所で同じブロックが拒否され、異なるブロックを承認する場合です。偶然発生した事象ですが、いつの日か、悪意を持った攻撃の結果として歯抜け現象が現れる可能性もあります。悪意を持ったユーザー1人（あるいはユーザー集団1つ）がネットワークの半分以上を乗っ取るような事態は、代償が高く付きすぎるからありえないと一般的には考えられています。しかし、ビットコインの価値が急上昇すると、そうとも言い切れなくなります。

2013年3月に起こった歯抜け事件はよく知られており、2つの異なるバージョンのビットコインプロトコルがノードで使用されていたことから起こりました（注4）。ビットコインがオープンソースのソフトウェアをベースにしている事実を思い起こさせる事件です。ビットコインとは、ビットコインユーザーが使用するものです。ビットコインの基本原則と初期バージョンはサトシ・ナカモト（注5）とのみ知られている人物の功績です。更新、バグの修正、改良などの作業は

一般的には、税金の支払を受け付ける形で

価値を認めてきました。国家はまた、

金銭に常に注意を払っています。金銭の主な役割の一つは、債権者の債務を帳消しにすることであり、これにより国家の本質的な機能の一つである司法監督と金銭が直結するからです。

これが、米国憲法が国会に対して「硬貨を鍛造し、外国硬貨も含めた価値を管理し、寸法や重量を規定する」権限を与えている理由です。ビットコインは国家権力とは無縁ですが、国家による保護を受けることもありません。ビットコインの利用が広まるにつれ、窃盗の機会も増えます。それでもビットコインが浸透する可能性はどの程度あるのでしょう？

**詐欺の懸念**

ビットコインの創立者であるサトシ・ナカモトが記した白書内で彼が述べている内容に即して言えば、取引手数料はもっぱら詐欺を防ぐために発生します。彼は、中央当局や「信頼のおける第三者」が関与することなく低コストで安全に支払が行えるシステムを提案しました。結果として、国家に依存しない価値単位という驚異的な発明が生まれましたが、それはあくまでも偶然でしょう。ビットコインへの関心のほとんどは、金銭は国家に独占されるべきではない、と説いたフレドリック・ハイエク（注6）からヒントを得ています。

手間の一つは匿名性が失われることです。仮想通貨の持ち主は

ビットコインユーザーのコミュニティが引き受けており、少数のプログラマーが大多数を占めます。ビットコインに対する

財布を持つ個人に連動しなければなりません。個人が所有できる財布の数には制限がないのは確かです。財布から所有者を特定することを難しくする方法はありますが、別途作業がかかります。ビットコインを利用するもう一つの手間は取引にかかる時間です。提案された取引がブロックチェーンに記録されるまでに、最低10分待たなければなりません。取引額が大きくなると、6ブロック（1時間）待つことも普通にあります。他の通貨を用いて電子的に小売取引を行う場合に比べて、非常に時間がかかります。（例えば、クレジットカードを店頭やオンラインで使用すると数秒しかかかりません。）ネットワーク上で大規模な金融取引を行えば、時間はさらにかかります。

ビットコイン取引を完了するにはどうしてこれほど時間がかかるのでしょう？ビットコインネットワークが分散型を採用していること（さらに、一種の多数決に依存していること）が根本の原因です。これは、最も特筆すべき特徴であると同時に、

熱狂的な歓迎の一部は、国家が発行する通貨に対する不信から来ているのは事実です。しかし、責任者が不在で、仲裁機能を欠き、償還請求も不可能なうえに、ほんの少数の人間しか理解できないほど複雑なコードで記述され、さらに少数の人間によって運営される通貨が主要通貨として流通している世界は、想像しがたいものがあります。

**国家の役割**

ビットコインのような信用通貨は、多くの人間が広範に受け入れている状況があってはじめて使い道が生まれます。理論的には、広く受け入れられている状況が生まれるためには国家は必要ありません。歴史的には、国家の後押しがなくとも普及した通貨の例はいくつかあります。だいたいの場合、国の通貨が不十分だった場合に発生しています。しかし、西洋の歴史においてはほとんどの場合、通貨には国家が関与してきました。少なくとも、国家は通貨を調停用の道具として用いてきました。

Charles L. Evans： *President*;、Daniel G. Sullivan： *Executive Vice President and Director of Research*、 Spencer Krane： *Senior Vice President and Economic Advisor*; David Marshall： *Senior Vice President*, *financial markets group*、Daniel Aaronson： *Vice President*, *microeconomic policy research*、 Jonas D. M. Fisher； *Vice President*, *macroeconomic policy research*、Richard Heckinger：*Vice President*, *markets team*、 Anna L. Paulson： *Vice President*, *finance team、* William A. Testa： *Vice President*, *regional programs*, *and Economics Editor 、* Helen O’D. Koshy および Han Y. Choi； *Editors*、

Rita Molloy および Julia Baker： *Production Editors*、 Sheila A. Mangler： *Editorial Assistant。*

*シカゴ連邦準備銀行ニュースレター* はシカゴ連邦準備銀行の経済研究部門により発行されています。本ニュースレターで反映される意見は著者のものであり、シカゴ連邦準備銀行や連邦準備金制度の意向を必ずしも反映しているわけではありません。

© 2013 Federal Reserve Bank of Chicago *シカゴ連邦準備銀行ニュースレター* の記事は、商業目的に用いられることなく、出典が適切に記載されている限りにおいて、その全体または一部の複製を許可します。その他にシカゴ連邦準備銀行ニュースレターの複製、配信、再発行、あるいは派生品の作成を行う場合、

書面による事前の許可が必要となります。T許可を得る場合は、編集主任であるHelen Koshyへご連絡ください。電話： 312-322-5830 または [メール： Helen.Koshy@chi.frb.org。](mailto:Helen.Koshy@chi.frb.org)*シカゴ連邦準備銀行ニュースレター* と他の銀行発行物の入手の際は以下をご参照ください： [www.chicagofed.org.](http://www.chicagofed.org/)

ISSN 0895-0164

彼は、金銭の生産は競争的な民間部門に任せるべきだ、と解説しています。しかし、この関連付けは的外れです。ビットコインは確かに政府の手から自由です（今のところは）。しかし、ハイエクが想像したものとは似ても似つかぬものに変貌しました。市場のおかげで通貨の価値が安定し、競争のある環境の中で私営企業が発行するわけではありません。ビットコインネットワークは自動的に作業をこなし、一定の間隔で通貨を新規発行しています。価値の安定した通貨、というハイエクが考案した「良貨」の定義からは見事に外れます。それだけではなく、先行者利益を得たことでデジタル通貨では半独占的な立場を得ており、

* 1. 連邦準備制度理事会からのデータに基づく著者の計算、 H.4.1 統計情報、 Visaファクトシート  [(http:/](http://corporate.visa.com/_media/)/[corporate.visa.com/\_media/](http://corporate.visa.com/_media/) visa-fact-sheet.pdf)、ビットコインチャート (www.bitcoincharts.com)を参照済。
  2. 因数分解するということは、素数の掛算として表現することを意味します。

ハイエクは通貨が国家に独占されるべきかどうかについては言及していません。

**結論**

現在に至るまで、交換媒体としてのビットコインの利用方法は制限されています。非合法活動を除けば、範囲はさらに狭まります。伝統的で規制を受けた手法の範囲外で資金を移動する方法として使われています。また、投機的な投資機会としても使われていると推定されます。ビットコインに賭けてみる人々が存在するのは、本格的な通貨に成長する可能性があるからです。ビットコインの特徴には、既存の通貨や決済システムに比べて不便な点もあります。

* 1. ミネアポリス連邦準備銀の総裁であるNarayana Kocherlakotaが提唱した「金銭＝記憶」概念との違いに注意してください：彼のモデルにおいては、金銭とは過去の取引内容の情報を具現化したものです。取引の当事者だけでなく、[取引対象も含んでいます。www.minneapolisfed.org/](http://www.minneapolisfed.org/) research/sr/sr218.pdfを参照してください。

特に、既存の通貨や決済方式で特に困っていない人々にとって、不便です。また、ハイエクや他の「オーストリア学派経済学」の学者が提案した内容を全て実現しているとは言えません。ビットコインが広く利用されるとすれば、政府による介入から自由でいる可能性は薄いでしょう。ビットコインのコードとネットワークの管理が不透明さに満ちており、脆弱であることだけでも充分な理由になります。それでも、ビットコインは観念的にも技術的にも目を見張る成果を挙げており、既存の金融機関で使用されたり（独自のビットコインを発行する可能性もあります）、政府自身が使用する事態もありえるでしょう。

4 [詳細は、 http://bitcoin.org/en/](http://bitcoin.org/en/) alert/2013-03-11-chain-forkを参照してください。

5 ビットコインの仕様を明記したサトシ・ナカモトの白書はここからダウンロードできます。 [http://bitcoin.org/bitcoin.pdf.](http://bitcoin.org/bitcoin.pdf)

6 参照先：F. Hayek, 1976, *Denationalisation of Money*, ロンドン：経済省