原文

<http://bitcoinmagazine.com/overcoming-moral-and-visceral-objections-to-bitcoin-good-and-bad-responses/>

**ビットコインに対する道徳的な、あるいは感情的な批判を乗り越えるために：模範解答と駄目な回答の紹介**

**著者：Vitalik Buterin**

たとえ現在ビットコインを使いこなしている者であっても、初めてビットコインのことを耳にした瞬間からまるごと受け入れたわけではないはずです。ビットコインに熱中している誰かをつかまえて最初にビットコインコミュニティに参加したときのことを聞いてみると、これがよくある話です：技術に詳しいネット市民がビットコインの話を聞きつけるけれどもシステムには深刻な欠陥があるのが明らかだしそのせいで数ヶ月後にはクラッシュをおこしそうだからやめておき、メディアで大々的に取り上げられたので数週間や数ヶ月後にもう一度確かめてみて、そこで初めて真剣に検討してみます。確かに、ビットコインはこれまでとは全く違うテクノロジーなので、最初から完璧に安心して扱う人がいるとは思えません。この記事の目的は、ビットコインを広めようとしている人々のために、よくある誤解を紹介し、ユーザーになりそうな人を説得する方法を解説することです。

**誤解その一：ビットコインには裏付けがない**

ビットコインに対する疑問でもっともよくあるのがこれです。内容は以下の通りです：現実の世界で私たちが慣れ親しんでいるものはほとんど、それ自体にはっきりとした利用価値があるからこそ、欲しいと思えるはずだ。リンゴを欲しがるのは健康に良くて美味しいからで、椅子を欲しがるのは快適だからで、パソコンを欲しがるのはネットで猫の画像を眺めるのに便利だからだ。取引や売買をするために必要だけど自分自身はいらないものを欲しがる場合でも、取引先のどこかにはそれを欲しがる人がいるという事実があるから、価値がある。ビットコインは違う。ビットコインはパソコンネットワーク上の数字にすぎず、それ自体には何の価値もない。石油に価値があるのは、石油会社に売ればガソリンが生成されてガソリンスタンドに売られ、車を運転する人がガソリンを購入して目的地に早く着けるからだ。ビットコインに価値があるとされるのは、ビットコインを誰かに売り、その誰かが別の誰かに売り、そのまた誰かに売り・・・と際限なく連鎖が続くからだ。しかし、それでは価値が生まれることがないし、そうした連鎖は社会的な約束事の上に不安定に乗っているだけなので、いつ崩壊しても不思議ではない。

**駄目な回答：ビットコインは経済全体が裏付けている**

上記の疑問に対するよくある答え方としては、「ビットコインに価値がある理由は、皆が支払い方法として受け入れているから」があります。たいてい、[価値は主観的](http://mises.org/austecon/chap4.asp)なものだという理論武装が続きます。要するに、何かに価値があるのは他の人がそれを欲しがる場合だけであり、それは事実上、人が欲しがるものであれば価値があるということを意味する、というものです。この答えは巧妙ですが、価値の連鎖に始まりや終わりが見えない、という当初の不安に何一つ答えていません。それどころか、巧妙な言葉のあやで問題をすり替えているだけです。この答え方をする人たちは概して、主観価値の学説によると内在価値など存在せず、本質的な価値を求めることは意味が無い、という話もしがちです。これも、少し異なる理由で間違っています。「内在する価値」の定義を２種類、一緒くたにしているのが間違っています。

内在価値の最初の定義は、全ての商品は融点や密度のように化学的あるいは非物質的な特性と呼べる魔法のような「価値」を内在しており、 私たちはそのポイントが高いからこそ価値を認めている、というものです。これは主観価値理論が既に論破しています。しかし、内在価値には、完璧に現実に即したもう一つの定義もあるのです。取引のためではなく、最終的な利用方法があるからこそ得られる価値のことです。リンゴや椅子やパソコンはどれも本質的な価値をしっかりと得ています。株式はこの定義を広義で満たしています（株式の配当を得られるし、会社が倒産しても払い戻しが得られるからです）。しかし、ビットコインにはこの定義は当てはまらず、それが問題となります。パソコンが99%値下がりすると買う動機が増しますが、ビットコインが99%値下がりすると取引上の利用価値が99%下がることを意味しますし、さらなる値崩れが起こらない保証もありません。

**模範回答その一：詳細を解説する**

ビットコインの価値を証明しようとすると堂々巡りになってしまう矛盾した状況を解決するには、有効なやり方が２種類あります。最初のやり方は、通貨が価値を維持する方法を詳しく紹介することです。論法は次の通りです。ビットコインに100ドルの価値があるとします。ボブはアリスにトースターを売る際に、代金としてビットコインを受け取ることに同意します。なぜボブはそれで問題がないのでしょう？アリスはそのビットコインを使ってチャーリーから椅子を買うこともできたはずだ、と知っているからです。アリスにはなぜそれがわかるのでしょうか？彼女はチャーリーがビットコインを受け取る姿を昨日、その前日、そのまた前日にも目撃しているからです。いきなりチャーリーが明日ビットコインでの支払いを拒否する可能性は極めて低い、とこれでわかるわけです。チャーリーはどうして明日もビットコインを受け取るのでしょう？なぜなら、上記と全く同じ理由により、ビットコインを使って日用品を買い、デーヴに代金を支払うことができるはずだ、と知っているからです。こうして、イブやフレッド、ジョージを経て、最後にザカリーがビットコインを使ってアリスから自転車を買うまで、全く同じ理由で取引が続きます。

一見すると、これは堂々巡りに見えるかもしれません。アリスがビットコインを受け取るのはボブが受け取っているからで、それが巡り巡って、ザカリーがビットコインを受け取るのはアリスが受け取るからだ、となるからです。しかし、これは論点の肝心な部分である、「時間」が受け持つ本質的な役割を見逃しています。人々がビットコインを受け取るのは、今日この時点で皆がビットコインを受け取っているからではありません。昨日の時点で皆がビットコインを受け取っていたからです。ゆえに、一旦ビットコインに価値が認められると、自己増幅の連鎖が始まり、理論的には永遠に価値が続くことになります。結果的に、この論法を用いればビットコインになぜ価値があるかについて強力な理由を述べることができ、問答に決着をつけることができます。

**模範回答その二：他の通貨だって一緒である**

ビットコインを非難から擁護するための、もう一つの回答方法はもっと単純で、擁護をそもそもしないことです。代わりに、他の通貨もビットコインと同じくらい危険だ、と指摘します。米ドルだと簡単にできますね。ドルにも本質的な価値がありません。アメリカ政府は税金の徴収に米ドルしか受け付けないから、ドルには絶対的な価値がある、と主張する人も確かにいます。しかし、この考え方には致命的な欠陥があります。政府が税金の支払いに米ドルのみを指定しているからといって、ドルの価値に底値が保証されているわけではないのです。どうしてなのかを知りたければ、例えばドルの価値が99%下落したと仮定しましょう（経済全体で100倍のインフレが起こったということです）。所得税はどう変化するでしょう？ドル換算での所得も100倍値上がりするので、税金上も100倍のドルを支払うことになります。つまり、もしドルで買えるモノやサービスが100分の1になれば、税金だって100分の1しか納められません。政府は、自国の通貨をコントロールできているわけではないのです。実質、社会の誰もと同じように、政府も通貨の奴隷にすぎません。

金（きん）は電子機器や装飾品などに利用できる本質的な価値があるので、もっと事情は複雑です。しかし、本質的な価値の割合は全体に比べるとかなり小さいので、無視できます。2001年の時点で、金は1オンス毎に300ドル以下の価値しかありませんでした。金の内在価値になんらかの影響力があるとすれば、その後の10年でオンス当り1900ドルまで金の値段が上がったので、電子業界や宝石商は6倍の価値を手にいれたことなり、現時点で値段が1300ドルまで下落したので彼らは絶対価値を求めて金を安く買い漁っているはずです。しかし現実はそうなっておらず、価値を貯蔵する役割という付加価値が付いていなければ、金のオンス当りの価値は最低100ドル程度まで下がっているだろうと主張する人々もいます。

**誤解その二：ビットコインはオタクによる貴族統治でしかない**

この反論は、地理的・金融的にもっと安定した通貨で今の通貨を置き換えられないか、と考えている人たちからよく来ます。不換紙幣は政府と銀行に大きな権力を与え、少数の選ばれた人たちによって管理されているわけだが、ビットコインは単に、親と同居しているような信頼できないプログラマーにその権力を渡すだけだろう、だからビットコインは以前からある不換紙幣より優れているわけではない、というのが彼らの主張です。並行してもう一つ、一般人はビットコインを司る複雑なアルゴリズムなど理解できるわけがないので、頭脳明晰な連中に支配されて抑圧されるのではないか、という反論もあります。プログラマーの観点からすると馬鹿げた主張ですが、「SHA256（ハッシュアルゴリズムの一種）」、楕円曲線暗号システム、Proof of Work (POW) プロトコルといった専門用語に触れ始めたばかりの人間からすると、心配になる人々の気持ちもわかります。

**及第点の回答：実際の仕組みを解説する**

ビットコインは複雑だと考える人は多いですが、実際に[近年](http://arxiv.org/abs/1008.1284)の[他の](http://link.springer.com/chapter/10.1007%2F978-3-642-13190-5_2#page-1)暗号化[プロトコル](http://zerocoin.org/)と比較するとビットコインは非常に単純にできています。以下、2段落だけでビットコインがなぜ安全なのか、全て解説できます。

ビットコインネットワークはあらゆる取引の記録を納めるデータベースを維持管理しています。この取引記録から、誰がどれだけビットコインを所持しているかがわかります。他人の口座を利用して取引を行うことを防ぐためには、公開鍵暗号法が用いられます。公開鍵暗号法では公開鍵と秘密鍵からなる一対の鍵が作成されます。秘密鍵を使用して「デジタル署名」を作成でき、公開鍵を使用すれば誰でもそれを確認できるので、秘密鍵の所有者から改ざん抜きで送信されたとわかります。ビットコインの所持者は秘密鍵を使用して自分のお金をやり取りする際に署名し、公開鍵を配布してネットワーク上で取引に問題がないことが確認されるようにします。

取引の順序も重要です。もしアリスがボブに10 BTC（ビットコイン単位）を送金したのち、チャーリーに対してもそっくり同じ10 BTCを送金しようとすると、ネットワークは前半ではなく後半の取引を拒否するべきでしょう。さもなければ、アリスがボブから10 BTCで商品を買い、続いて全く同じ10 BTCを用いてチャーリーからも商品を買おうとした場合、ネットワークはボブへの送金を中止してしまい、結果的にボブから10 BTCをだまし取ることになってしまいます。この問題を解決するため、ビットコインは「ブロックチェーン」という仕組みを利用しています。特定のユーザーたち（「採掘者」と呼ばれます）がプログラムを走らせ、取引記録を「ブロック」と呼ばれるパケットに変換します。正式なブロックを複製するのは非常に困難です。あまりに困難なので、ネットワークを通じて平均10分に一回しかブロックが作成されないよう自動的に調整されています。各ブロックは直前のブロックへのポインタを含んでおり、「ブロックチェーン」を構成しています。もし二つの異なるブロックチェーンが存在する場合、より長い方が正式なものとみなされます。ブロックの内容を書き換えると必ずブロックは無効になります。理由は、ブロックの有効性を保証する数学アルゴリズムは非常に複雑にできており、たとえ1ビットだけブロックの内容を変更した場合でも、ブロックを再度有効にするにはほぼ全て作り直さなければいけないからです。作業を全てやり直すとブロックは大幅に書き換えられ、直後のブロックもそのブロックへポインタを参照しているゆえに作り直すことになり、作り直しの連鎖が続きます。ゆえに、もしアリスが10 BTCを二重に使用しようとすると、彼女はボブへ10 BTCを送金するよりも前から新しいブロックを作成し、ネットワークが新しいブロックを追加するよりも先にネットワークに追いつかなくてはなりません。個人レベルではほぼ不可能な作業です。

一度に全て理解するのは難しいでしょう。[サトシ・ナカモト（ビットコインの創設者の一人）の論文](http://bitcoin.org/bitcoin.pdf)に概念がより詳しく書かれています。しかし、驚くでしょうが解説にはほとんど数学的な内容はありません。公開鍵暗号法の性質を理解するだけですみます。一方で、現在開発されている暗号化アルゴリズムで真に革新的なものはほとんど、アルゴリズムのステップを理解するだけでも大学の数学課程の学位が必要なレベルです。ビットコインの場合、 基本を成す暗号化の仕組み（公開鍵と秘密鍵の作成に楕円曲線暗号システムを使用し、SHA256ハッシュアルゴリズムを使用して高度に「入り組んだ」ブロック認証システムを作成）が安全であるかどうかの確認は確かに数学者に頼る必要があります。しかし世界中の数百もの大学で安全性が個別に研究されており、基本技術は安全である、との意見で全て一致しています。この時点で、SHA256 と楕円曲線暗号システムの安全性、つまり「こうやって動作しています」の部分についての解説は一休みします。そういうわけで、この次の段落で解説する回答のほうがもっと良いでしょう。（それでも、ビットコインの仕組みや暗号化が数学的にいかに素晴らしくできているかについて啓蒙する努力は怠らないでください）

**模範回答その一：数学者は談合などしていない**

政府の強制力、銀行の社会的地位、それにビットコインに関するあらゆる「専門家」の持つ数学やコンピューター工学の知識を比較すると、ある一点で異なります。数学オタクとコンピューター工学オタクは同じ集団内に属さないどころか、どんな類の集団にも属していない点です。世界中の政府は特定のフォーラムで会談を開き、銀行は業界内で会議を開催して富裕層向けに会員制イベントを開き、両者は中央銀行制度や金融規制システムを通じて深い交流を行っています。一方、数字とギリシャ文字の魔法使いたちは世界中の大学に散らばって存在しています。デジタル世界の専門家はオープンソース開発集団や企業や近所の天才少年など、いたるところにいます。こうした集団が社会征服を企んでいると言うのは、鍛冶屋や刀鍛冶が中世の時代に軍隊を掌握しつつあった、と言うのと同じくらい荒唐無稽な話です。

さらに、数学者やプログラマーの集団は誰にも開かれている一方で、政治家や銀行のシステムに参加するには莫大な富を既に所有し、運を味方につけて人脈を蓄える必要があります。オンラインで[公開](http://mooc-list.com/)されている[何百](http://cousera.org/)もの[講座](https://www.edx.org/)を[無料](http://udacity.com/)で利用すれば誰でも数学やコンピューター工学を学べます。YouTubeやデジタル書籍、専門書や図書館でさらに深く学ぶこともでき、自分自身や親が中産階級付近にいれば（アメリカ外であれば）大学で学ぶこともできます。コーセラ（オンライン教育団体）で「エリート銀行家になる方法」を探しても見つかりはしないでしょう。

**模範解答その二：不換紙幣だって技術的に複雑である**

もう一つの反論方法は、繰り返しになりますが、ビットコインを擁護するのではなく不換紙幣の短所を指摘することです。多くの人々が、不換紙幣は単純だと間違った考えを持っています。ドルを送金して数字を打ち込めばクレジットカードで支払いができますが、ビットコインはプログラムや暗号化やSHA256が絡んでくるので、難しい：違いますか？ここでの誤解ははっきりしており、通貨の正しい理解は、本当は２段階（次元）に分けて行う必要があるという点です。ビットコインはそのどちらにおいても優秀であると言えます。低次元の理解は、実際に使いこなすにはどうすればよいかというレベルです。ビットコインは単純です。「送金」をクリックすれば送金でき、受け取りたい場合はビットコインアドレスをコピー＆ペーストすれば済みます。クレジットカードのほうがより複雑に見えます。個人情報を大量に記入し、「支払取り消し」の仕組みを理解し、毎月の請求額を支払って必要であれば利息も払い、それに加えて、なぜかオンライン外のクレジットカード利用ではレシート（またはパソコン画面）にサインする必要があります。現金で支払う場合は、金額に応じておつりを暗算する必要があります。

通貨について高次元で理解する場合、ビットコインには確かに採掘やらブロックチェーン集団やらクライアントソフトのパッチアップデートやらがついてまわります。しかし、不換紙幣自体にも煩雑さが内蔵されています。ビットコインでは、100ビットコインを所持していれば、それは単に100ビットコインを所持しているだけの話です。しかし、銀行口座に100ドルを所持しているということは何を意味するのでしょうか？技術的に正しい回答は、銀行が100ドルあなたから借りており、政府が銀行の破産時に備えて最大25万ドル程度まで預金を保証しているということです。銀行自身は、ほんのわずかな量の現金と「外貨準備」という名の銀行間取引でのみ有効な通貨制度で自らを保護しています。しかし、預金のほとんどは銀行が貸し出しており、借り手はそのお金を恐らく使い果たしているでしょう。その使われたお金は別の銀行に預金として入れられており、結局は同じ現金が複数の銀行に預金として入れられているということになります。ここからがさらにややこしい点なのですが―そして上記のビットコインについての解説と公平に比較するなら、クレジットカードの問題にはまだ触れてすらいないのですが―銀行のATMやSWIFTコードだって暗号化をかけられて保護されています（実際にはかなりの場合、本物の暗号化の代わりに線形代数と差分方程式を用いた機械アルゴリズムを用いてセキュリティが確保されています）。総合すると、ビットコインと不換紙幣の複雑さは、同程度であるようです。

**誤解その三：ビットコインは有限であり、いつか枯渇する**

問題点は以下の通りです。現存するビットコインは有限であり、正確には2100万個存在し、時間が経てばいずれビットコインは全て失われるのでシステム全体の価値が消える、という考え方です。通貨の供給量が有限であることはかなり心配されており、経済モデルにつきもののデフレの心配もあります。ここでは、そういった心配事に直接答えることはしません。代わりに、最初に提起された問題に着目します。

以下は模範的な回答になり得ます。一定時間が経過してビットコインの半分が仮に失われたとすると、需要と供給の関係から、残りのビットコインの価値が二倍に上がります。それゆえ、各自が所持して取引しているビットコインは平均して半分になります。さらに同じ時間がたつと、市場に出回るビットコインの量は元の四分の一になります。その次は八分の一に、次は十六分の一に、と続きます。しかし、ここが肝心なのですが、どれだけ繰り返してもビットコインの量がゼロになることはありません。ビットコインのプロトコルを変更して量を増やすことはいつでも可能で、そうした事態には恐らくそれが起こるでしょう。もう一つの模範的な回答としては、そんなに大量にビットコインが失われる事態はまずありえないだろう、というものです。損失が深刻なレベルに達するのなら、安全保護システムが開発されてそういった事態を防ぐことになるでしょう。最後の手段としては、一定の速度で無限に増殖可能な通貨を新たに作り直してこの問題を解決することが可能です。その場合、一定の割合で通貨量が失われることを前提にして通貨供給量の総額が決められます（例えば、一年に100万コインが流通して年間1%の損失レートだとすると、1億コインが総量になります）。結論としては、この問題を回避する方法はいくらでもあるので、特に問題にする必要もないということです。

**誤解その四：ビットコインはねずみ講である**

ビットコインを紹介されると、多くの人は即座にねずみ講だ、と結論づけます。理屈はこうです。ビットコインは値上がりする投資物件として売られているが、値上がりが続くためにはより多くの人が参加し続ける必要がある。ビットコインに新規参加者がいなくなれば、全体の仕組みが崩壊するだろう、です。

最も一般的な反論方法は実のところ模範的回答でもあります。典型的な「駄目な回答」の要素も少し含んでいるのですが。詳細は以下の通りです。ねずみ講は中央に権力が集中しており、各ユーザーは己の下に新規参加者を呼び込むことで利益を得られる構造になっています。仕組みそのものが詐欺と曲解で出来上がっています。例えば、ねずみ講は自らをねずみ講とは呼びません。一方、ビットコインは権力が分散しており、オープンソースで、各ビットコイン所持者は新規参加者を呼び込んでもほんの少ししか利益を得られません。「駄目な回答」に陥るのは、ビットコインとねずみ講の違いについて学術的に解説をし始めたときです。批判的な人たちは、権力が分散しているかどうかは関係なくてビットコインの複雑さが既に詐欺の代わりを果たす、と主張します。これまでに解説した通り、それは完全に間違っているのですが、それでもビットコインの信憑性を「ねずみ講」から「市場操作」へ軽減する程度の効果しかありません。

この論法がどうして「模範解答」になり得るのかは、次の点をはっきりさせた時にわかります。ねずみ講や市場操作と違って、ビットコインは真に革命的な特性を備えており、ビットコインユーザーのほとんどはお金儲けよりももっと大切なものを求めて参加している、という点です。ビットコインを使えば世界中へほとんど手数料をかけずに送金でき、ほぼ匿名のままで行え、規制もありません。それだけでもとても魅力的なことなのに、権力分散型の構造まであります。より正確には、ビットコインはスタートアップ企業のようなもので、2100万単位のビットコインは株式のようであると言えます。むろん、ビットコインはほぼ匿名かつ無料、規制を受けずに世界中に即座に送金可能な通貨という重要な役割を担っているので、厳密にはその定義は正しくはないのですが。ビットコインのコミュニティに参加するということはそれだけでビットコインを「信頼」していることになります。たとえ自分ではビットコインを所持していなくても、ビットコイン経済がうまく周り、既存のビットコインビジネスが軌道に乗れば、間接的に利益は得られます。スタートアップ企業の例えが気に入ったならば、参加してみてはいかがでしょう。参加しないのもありです。私たちは変わらず、この小さな分散型スタートアップを育てる最大限の努力を続けるだけです。