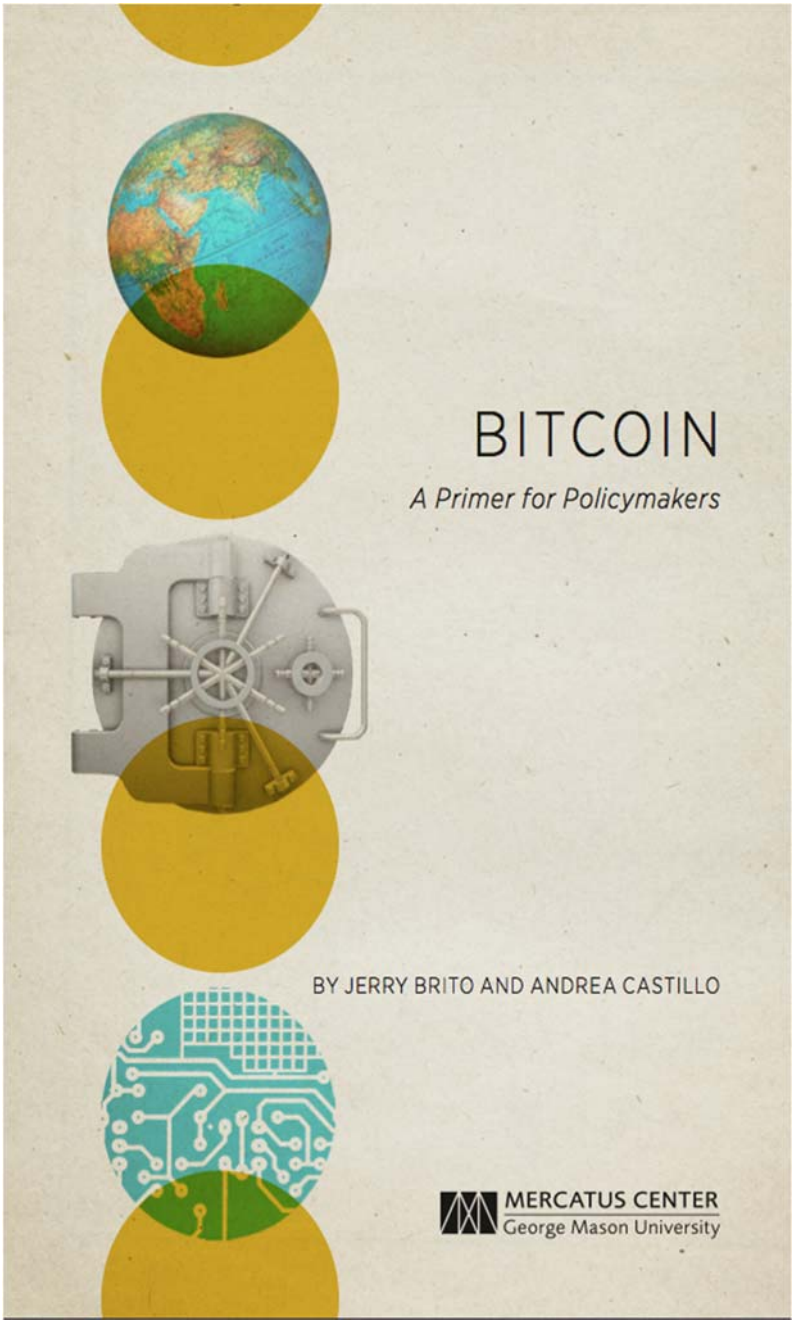
BITCOIN
A Primer for Policymakers
BY JERRY BRITO AND ANDREA CASTILLO
MERCATUS CENTER
George Mason University

ビットコイン
政策立案者のための入門書
ジェリー・ブリート／アンドレア・カスティーヨ　著

メルカトスセンター
ジョージ・メイソン大学
3351 Fairfax Drive, 4th Floor
Arlington, VA 22201-4433
(703) 993-4930
mercatus.org

ビットコインは世界初の完全な権力分散型のデジタル通貨です。たった四年前まで、ビットコインのことを知っていたのはインターネットのフォーラムに集う一握りの愛好家だけでした。今日では、ビットコイン経済は小さな国家の経済規模をしのぐほどになっています。ビットコイン（またはBTC）の価値は大きく上がり、また変動しました。初期には数セント程度の価値だったのが、ピーク時の2013年4月には260ドル以上になっています。現時点のビットコイン経済の時価総額は総額10億ドル以上と推定されています。[1] 大小の企業がビットコインのシステムを業務に組み入れ、ビットコイン経済内で新しいサービスを提供することに興味を示しています。ベンチャーキャピタリストもまた、この成長中の産業に投資しようとやっきになっています。[2] ビットコインの開発経緯と初期の成功は、現代起業家の創造力の証でもあります。

1.bitcoincharts.comで提供される財務情報によると、合計時価総額は2013年5月29日時点で1,457,815,292ドルと推定されています。
2.Sarah E. Needleman、Spencer E. Ante：「Bitcoin Startups Begin to Attract Real Cash」　ウォール・ストリート・ジャーナル、2013年5月8日
http://online.wsj.com/article/SB10001424127887323687604578469012375269952.html

ビットコインは権力分散型をとっているため、半匿名的に使用できます。このおかげで、規制機関の目に留まることになりました。ビットコインを支払い用のシステムとして魅力的にしている資質は、その一方で脱税や資金洗浄、非合法な商品の取引も可能にします。米国財務省の金融犯罪執行ネットワーク(FinCEN) [3]と司法省[4]はビットコインを含む仮想通貨の規制に関して公式な声明を発表しました。仮想通貨に関する米国会計監査院の報告書は、国税庁に対して、ガイドラインを発行することで税法遵守上のリスクを減らすよう勧告しました。[5]報告書の付録には国税

庁の次長であるスティーブン・T・ミラー（Steven T. Miller）からのレターが記載されています。彼は、国税庁が「リスクに対処するよう努力している」と監査院に約束しています。その上、商品先物取引委員会の理事が最近、ビットコインが委員会の管轄に含まれるかどうかを調査することに前向きな姿勢を見せました。[6]この未だ黎明期にある技術を最善な方法で監督するために、革新的な金融プラットフォームが前途有望に成長する可能性を二重三重に指令を下すことでつぶさないよう、政府の規制機関は注意する必要があります。

3.アメリカ合衆国財務省金融犯罪執行ネットワーク：「Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies」（規制ガイドライン、FIN-2013-G001、アメリカ合衆国財務省、ワシントンD.C.、2013年3月18日）http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
4.Jennifer Shasky Calvery：「Combating Transnational Organized Crime: International Money Laundering as a Threat to Our Financial Systems」（司法に関する下院委員会内の、犯罪・テロリズム・国土安全保障に関する小委員会で記録された証言、2012年8月）http://www.justice.gov/ola/testimony/112-2/02-08-12-crm-shasky-calvery-testimony.pdf
5.米国会計検査院：「Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Compliance Risks」（金融に関する上院委員会への報告、GAO-13-516、2013年5月）http://www.gao.gov/assets/660/654620.pdf
6.Tracy Alloway、Gregory Meyer、Stephen Foley：「US Regulators Eye Bitcoin Supervision」フィナンシャル・タイムズ、2013年5月6日http://www.ft.com/intl/cms/s/0/b810157c-b651-11e2-93ba-00144feabdc0.html

この入門書を通じて、ビットコインネットワークの属性、仕組み、半匿名な性質を手短に紹介します。ビットコインネットワークを発展させ進歩させることの利点を解説しつつ、消費者や政策立案者、規制機関にとっての懸念も取り上げていきます。現在の規制状況を説明し、将来施行される可能性のある規制についても見ていきます。締めくくりとして、政治家の懸念を和らげつつ、ビッ

トコインネットワーク内にイノベーションの余地を残せるよう、政策提言を行います。

ビットコインとは何でしょう？

ビットコインはオープンソースの、ピアツーピア方式で運営されるデジタル通貨です。ビットコインをユニークたらしめている要素は多くありますが、その中でも、世界初の完全に権力が分散化されたデジタル決済システムという点は特筆すべきです。複雑に聞こえますが、基礎を形作る概念を理解するのは難しくありません。

概要

サトシ・ナカモトという名前で知られる正体不明なプログラマーによって2008年にビットコインが発明されるまで、オンライン取引の際は常に、信頼できる第三者が仲介を果たす必要がありました。例えば、アリスがボブにインターネット経由で100ドルを送ろうとすると、ペイパルやマスターカードのような第三者サービスに頼る必要がありました。ペイパルのような仲介業者はアカウント主の残高を台帳に記録しています。アリスがボブに100ドルを送金すると、ペイパルは彼女のアカウントから代金を引き落とし、ボブのアカウントに追加します。

そういった仲介業者がいないと、デジタル通貨は二重に使用される可能性があります。台帳を記録する仲介業者がいないと想像してみてください。デジタル文書がただのコンピューター上のファイルにすぎないように、デジタル通貨もただのファイルにすぎま

せん。アリスはマネーファイルを添付したメッセージを送信することで、ボブに100ドルを送金することだってできます。しかし、メールと同様に、資料を添付するだけだと、その資料そのものはパソコンから消去されません。アリスはマネーファイルを送信した後も、ファイルのコピーを保持しています。そうすると、彼女は同じ100ドルをチャーリーに送ることだって簡単にできます。コンピューターサイエンスの分野では、これは「二重使用」問題[7]として知られ、ビットコインが登場するまでは信頼できる第三者に台帳を記録してもらうことでしか解決できませんでした。

7.David Chaum：「Achieving Electronic Privacy」サイエンティフィック・アメリカン、1992年8月号、96-101ページ

ビットコインの発明が革新的なのは、第三者を必要とせずに二重使用問題を解決する方法を初めて編み出したからです。ビットコインは、ピアツーピアネットワークを通じてビットコインシステムのユーザー全員に台帳機能を分散させることでこれを実現しました。ビットコイン経済内で行われる取引は全て、ブロックチェーンと呼ばれる公開済みで分散型の台帳に記録されます。新規取引はブロックチェーンに参照され、同じビットコインがまだ一度も使用されたことがないかどうかチェックされます。これにより、二重使用の問題を解決します。全世界にまたがり、数千のユーザーから構成されるピアツーピアネットワークが第三者の役割を果たし、アリスとボブはペイパルの力を借りずに送金できます。

真っ先に注意するべきなのは、ビットコインネットワーク上の取引はビットコイン建てで行われており、ペイパルのようにドルやユーロや円建てされているわけではない点です。この特徴のおかげで、ビットコインは権力分散型の決済ネットワークであるだけ

でなく、仮想通貨ともなりえます。ビットコイン通貨の価値は金（きん）や政府が発行する不換紙幣に依存するのではなく、皆がどれだけ通貨に価値を認めているかによって決まります。ビットコインのドル価格は、各国通貨の為替レートと同様に、オープンな市場で決定されます。[8]

8.「Markets」 Bitcoincharts.com、2013年7月30日にアクセスhttp://bitcoincharts.com/markets/

仕組み

ここまでは、ビットコインが一体何であるかを解説してきました：権力分散型のピアツーピア決済ネットワークであり、オンライン上に存在する現金として実質的に機能する仮想通貨です。ここからは、ビットコインがどう機能しているかについて、詳しく見ていきます。

公開鍵暗号方式を巧みに利用することで、取引を認証して二重使用を防ぐ仕組みがとられています。[9]公開鍵暗号方式では、各ユーザーに二組の「鍵」が与えられます。ひとつは秘密鍵と呼ばれ、パスワードのように個人の秘密とされます。もうひとつは公開鍵と呼ばれ、誰とでも共有できます。アリスがビットコインをボブに送金する際、彼女は「取引」と呼ばれるメッセージを作成します。そこにはボブの公開鍵が埋め込まれており、アリスは自分の秘密鍵を利用してメッセージを「署名」します。アリスの公開鍵を見れば、取引が彼女の秘密鍵を用いて行われたと誰でも確認できます。正当な取引であり、資金の新たな持ち主はボブになったことも確認できます。取引（つまり、ビットコインの持ち主の移り変わり）は記録され、タイムスタンプが押され、ブロック

チェーン内のある「ブロック」に表示されます。公開鍵暗号方式のおかげで、ネットワーク内の全てのコンピューターではビットコインネットワーク内の全取引記録が常に更新されて認証されます。これにより、二重使用と詐欺行為が防止できます。

9.Christof Paar、Jan Pelzl、Bart Preneel：「Introduction to Public-Key Cryptography」、Christof Paar、Jan Pelzl著「Understanding Cryptography: A Textbook for Students and Practitioners, ed.（New York: Springer, 2010）」第六章
サンプルは以下にて閲覧可能：http://wiki.crypto.rub.de/Buch/download/Understanding-Cryptography-Chapter6.pdf

「ネットワーク」が取引を認証し、台帳の勘定を合わせると言うとき、一体何を意味しているのでしょうか？また、新しいビットコインはどのようにして作られ、通貨の供給に組み入れられるのでしょうか？これまで見てきたように、ビットコインはピアツーピアネットワークであるため、通貨を作り出したり取引を認証する当局は存在しません。取引を記録して勘定を合わせるため、ネットワークはユーザーから提供されるコンピューター処理能力に頼っています。こうしたユーザーは、貢献度に応じて新しく作成されたビットコインを報酬として受け取るため、「採掘者」[10]と呼ばれます。ビットコインは、ブロックチェーン内の取引を認証する複雑な数式を数千ものコンピューターが分散して処理する過程で作成、つまり「採掘」されます。ある解説者が指摘したとおり、

> ビットコインの実際の採掘過程は純粋に数式処理で成り立っています。素数の検索を例にとるとわかりやすいでしょう。小さな素数は比較的簡単に見つかります（古代ギリシャのエラトステネスは素数発見のアルゴリズムを世界に先駆けて作り上げていました）。しかし、発見が続くにつれ、

大きな素数を見つけるのは困難になっていきます。今日では、研究者は素数を発見するために先進の高性能コンピューターを使用しており、結果は数学コミュニティ内で評価されます（例えば、テネシー大学では最も大きな素数5,000個の一覧を管理しています）。
ビットコインでは素数の検索は行うわけではなく、代わりにビットコインの「ハッシュ」アルゴリズムを適用した際に特定のパターンを生成するデータ列（「ブロック」と呼ばれます）を探します。パターンの一致が確認されると、採掘者はビットコインで報酬を得られます（もしそのブロックが取引の認証に使用されれば、手数料も得られます）。得られる報酬の大きさは、ビットコインの採掘が進むにつれて減っていきます。
検索の難しさも増すので、パターンの一致を見つける処理の複雑さも増します。この二つの要因により、ビットコインが生成される率は時間が経つにつれ減っていき、金のような商品の生産率に類似していきます。ある時点で、ビットコインは生成されなくなり、採掘者のインセンティブは取引の手数料だけになります。[11]

10.採掘者はただのコンピューターオタクであることが多いのですが、採掘が困難で高価になるにつれ、採掘活動はプロの領域に移行していくでしょう。
詳細は次を参照してください。Alec Liu：「A Guide to Bitcoin Mining」、Motherboard社、2013年3月22日http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600
11.Ken Tindell：「Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995」ビジネス・インサイダー、2013年4月5日http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4

通貨ネットワークを維持して認証するためのインフラを管理するために十分なコンピューター処理能力が各々の採掘者から提供さ

れるよう、プロトコルが設定されています。採掘者は、ネットワークを維持してブロックチェーン内の取引を認証するためにコンピューター処理能力を提供することで、新しく生成されたビットコインを報酬として受け取ります。採掘に当てられる処理の割合が多くなると、プロトコルは数式処理の難易度を引き上げます。これで、ビットコインが常に予測可能で限定された率でのみ採掘されるようにしています。

このビットコイン採掘プロセスは永遠に続くわけではありません。ビットコインは金や他の貴金属を地中から採掘する過程を模倣するように設計されました。有限で、既知数のビットコインしか採掘されないようになっています。任意に定められた上限は2100万ビットコインです。採掘者は2140年に最後の「サトシ」、あるいは0.00000001ビットコインを大変な苦労を経て採掘し終えるだろうと予測されています。採掘に当てられるコンピューター処理量が高まれば、採掘の難易度も上がるため、この最後の「サトシ」を得るのはデジタル処理上、極めて難易度の高い作業になります。最後のサトシが採掘されれば、採掘者はコンピューター処理能力を取引の認証に割り当てる報酬を、新規採掘されたビットコインではなく取引手数料で受け取ることになります。これにより、最後のビットコインが採掘された後でも、採掘者にとってはネットワークを維持させるインセンティブが与えられます。

半匿名性

メディアがビットコインに着目する点の中でも、デジタル通貨によりユーザーが匿名性を獲得できることが特に大きくとりあげられています。しかしながら、この考えはビットコイン通貨を誤解した結果生まれたものです。

オンライン取引は今日にいたるまで第三者の仲介を必要としてきたため、匿名ではありませんでした。例えば、アリスがペイパルを通じてボブに送金すると、ペイパルは毎回記録を取ります。アリスとボブのペイパルアカウントは各自の銀行口座に連動しているため、彼らの身元は恐らく知られているでしょう。一方で、アリスがボブに現金で100ドル渡せば、仲介業者は存在せず、取引の記録も残りません。アリスとボブがお互いの正体を知らなければ、取引は完全に匿名ということになります。

ビットコインは二つの両極端の中間に位置します。ビットコインは、ある一面では現金のように機能します。アリスがボブにビットコインを渡すと、アリスの手元からビットコインが消え、ビルの手元に残ります。彼らの身元を知る第三者による仲介もありません。別の一面では、現金取引と異なってブロックチェーン内に取引が行われた公開鍵、日時、金額、その他の情報が記録されます。実際、ビットコイン経済で過去に行われた取引は全て、ブロックチェーン内で公開されて閲覧可能です。[12]

12.経済研究家にとっては、朗報であることに注意してください。

全ての取引について公開鍵（「ビットコインアドレス」とも呼ばれます）[13]がブロックチェーン内に記録されていますが、公開鍵自身は誰の身元にも結びついていません。しかし、ある個人の身元が公開鍵に結びついている場合、ブロックチェーン内に記録された取引を見るだけでその鍵に関連した全ての取引が簡単に閲覧できます。そのため、第三者や取引相手に対して身分を明かすことなく取引が行えるという点でビットコインは現金に非常によく似ているのですが、特定のビットコインアドレスから送金された、あるいは送金される取引が全て追跡可能である点は現金と

異なります。この点から、ビットコインは匿名ではなく、半匿名と言えます。

13.ビットコイン　ウィキ、見出し：「Address」2013年7月30日にアクセスhttps://en.bitcoin.it/wiki/Address

半匿名のビットコインアドレスから実社会の身元を割り出すのは、想像されているほど難しいことではありません。ひとつには、個人の身元（少なくとも、IPアドレスのような身元を割り出せる情報）はその個人がウェブサイト上でビットコイン取引を行ったり、ビットコインの両替所でドルに交換した際に記録されることがよくあります。

半匿名でいられる確率を増やすためには、Torのような匿名化ソフトウェアを利用し、身分を追跡されるおそれのあるビットコインアドレスを用いて取引をしないよう気をつける必要があります。

最後に、ブロックチェーンを眺めるだけでも身元を割り出すことは可能です。ある研究結果によると、ビットコインをシミュレーションし、行動ベースのクラスタ手法を利用して実験を行った結果、40%のビットコインユーザーの身元が判別可能であるとされています。[14]ビットコイン取引グラフの統計的な性質を早期分析した結果は、適切なツールを用いて受動的にネットワーク解析を行えば、ビットコインユーザーの金融活動や身元を暴くことができることを示しています。[15]より大きなデータセットを利用してビットコイン取引グラフの統計的な性質を後期分析した結果からも、同様な結論が得られました。[16]

14.Elli Androulaki、その他：「Evaluating User Privacy in Bitcoin」、IACR暗号化ePrintアーカイブ 596 (2012年)http://fc13.ifca.ai/proc/1-3.pdf
15.Fergal Reid、Martin Harrigan：「An Analysis of Anonymity in the Bitcoin

System」、Yaniv Altshulerその他編集「Security and Privacy in Social Networks(New York: Springer, 2013)」http://arxiv.org/pdf/1107.4524v2.pdf
16.Dorit Ron、Adi Shamir：「Quantitative Analysis of the Full Bitcoin Transaction Graph」、IACR暗号化ePrintアーカイブ 584 (2012)http://eprint.iacr.org/2012/584.pdf

ビットコイン取引グラフを解析した別の結果では、「エンティティ・マージ」手法[17]を使えば観察者がユーザーの行動から構造的なパターンを見出すことが可能であることが再度確認され、「ビットコインの匿名性を脅かす最も大きな脅威の一つである」と強調されました。[18]それにも関わらず、ビットコインユーザーは従来のデジタル送金サービスのユーザーよりはるかにプライバシーが守られています。従来のサービスでは、取引を行う第三者の金融仲介業者に詳細な個人情報を渡さなければなりません。

17.エンティティ・マージとは二つ以上の公開鍵を同時に一つの取引へ入力する行為を観察する過程です。これにより、ユーザーが異なる公開鍵を複数所有していても、観察者は徐々にそれらを関連付け、複数の公開鍵による見せかけの匿名性を取り除くことが可能です。
18.Micha Ober、Stefan Katzenbeisser、Kay Hamacher：「Structure and Anonymity of the Bitcoin Transaction Graph」、Future Internet 5、2013年第二号http://www.mdpi.com/1999-5903/5/2/237

ビットコインは「匿名」な通貨と称されますが、実際には、ビットコインネットワーク内で匿名でいるのは非常に困難です。公開台帳に記録された取引が半匿名であっても、取引から数年後に身元を特定することだって可能です。

ビットコインの仲介業者が、伝統的な金融仲介業者に義務付けられた銀行秘密法の規制に全て適合した場合、匿名性が保証される可能性がさらに低くなります。ビットコイン仲介業者に顧客の個人情報を収集する義務が課せられるからです。

利点

ビットコインについて勉強し始めた人の多くが最初に口にする疑問は、ドルが使えるのにどうしてビットコインを持つ必要があるのだろう？です。ビットコインはまだ新しく、不安定な通貨であり、多くの業者が扱っているわけではありません。ビットコインの利用法はほとんど実験段階にとどまっているように見えます。ビットコインを使いたくなる理由を理解するためには、伝統的な通貨の代替としてではなく、新しい決済システムとしてとらえるのが有効でしょう。

低い手数料

第三者の仲介が入らないため、ビットコイン取引は伝統的な決済ネットワークより大幅に安く、素早く行えます。取引が安く済むため、小額決済に使用したり、他の利用方法が可能になります。さらに、ビットコインは中小企業や国際送金の手数料を下げる方法として大きな可能性を持っています。資金へのアクセスを楽にして国際的に貧困を減らし、資本規制や検閲から個人を守り、抑圧された集団の資金情報を守り、（ビットコインプロトコル上と、内部の両方で）イノベーションに拍車をかけます。一方で、ビットコインの権力分散型の性質は犯罪のチャンスも引き寄せます。ここでの課題は、ビットコインの利点を維持しつつ、犯罪に使われる機会を減らせるプロセスを構築することです。

まず、ビットコインは商売上の決済費用を抑えようとするコストに敏感な中小企業にとって魅力的です。クレジットカードは決済を大幅に簡素化しましたが、業者にしてみれば大幅にコストが上

乗せされます。顧客がクレジットカードで支払いできるようにしたい業者は、まず各クレジットカード会社に業者アカウント費用を支払う必要があります。各クレジット会社との契約内容に応じて、企業は様々な認証費用、取引費用、明細書発行費用、交換費用、カスタマーサービス費用などを支払わなければなりません。これらの費用はすぐに積みあがり、商売のコストを大幅に増やします。しかし、業者がコスト節約のためにクレジットカード決済をあきらめると、クレジットカードの便利さを享受したい顧客からの売り上げを大幅に失うことになります。

ビットコインは第三者を必要とせず直接取引を行えるため、クレジットカード取引にまつわる高価な手数料を節約できます。ペイパルやフェースブックで知られるピーター・シエル（Peter Thiel）に率いられたベンチャーキャピタル、ファウンダーズ・ファンド（Founders Fund）は最近、決済処理会社のBitPayに300万ドルを投資しました。同社が国境を越えてオンライン交易のコストを下げられるからです。[19]実際、中小企業は既にクレジットカード会社とのビジネスコストを節約するため、ビットコインの受付を始めています。[20]その他の企業も、取引を素早く、効率よく行えるという理由からビットコインを受け付け始めています。[21]より多くの人がビットコインを利用し始めるにつれ、ビットコインを利用したビジネスの取引手数料は下がり続けるでしょう。

19.Tom Simonite：「Bitcoin Hits the Big Time, to the Regret of Some Early Boosters」、 MITテクノロジー・レビュー、2013年5月22日http://www.technologyreview.com/news/515061/bitcoin-hits-the-big-time-to-the-regret-of-some-early-boosters/
20.Gabrielle Karol：「Small Business Owners Say Bitcoins Better Than Credit
Cards」 FOXビジネス・スモールビジネスセンター、2013年4月12日http://smallbusiness.foxbusiness.com/entrepreneurs/2013/04/12/small-business-ow

ners-say-bitcoins-better-than-credit-cards/
21.Bailey Reutzel：「Why Some Merchants Accept Bitcoin Despite the Risks」Payments Sourceサイト、2013年5月21日http://www.paymentssource.com/news/why-some-merchants-accept-bitcoin-despite-the-risks-3014183-1.html

クレジットカードでの決済を受け付けると、支払拒否を利用した詐欺にかかる可能性があります。企業は長い間、詐欺的な「支払拒否」、または商品が届いていないという虚偽の申告を盾に消費者が支払の取り消しを要求する行為に悩まされてきました。[22]そのような詐欺の一例として、ボブがCraigslistに掲載したノートパソコン売り払い広告に対して、アリスがボブにペイパル経由で支払を行うケースがあります。アリスはボブの家を訪れ、ノートパソコンを手に入れた後、「支払拒否」（支払の差し戻し）を要求します。ペイパルは支払拒否をキャンセルするためには出荷証明を要求しますから、ボブには打つ手はありません。それにより、企業は商品そのものと、商品に支払われた代金、それに支払拒否の手数料を失うはめになります。非可逆な決済システムとして、ビットコインは消費者による支払拒否がもたらした「マイルドな詐欺」を無くすことができます。中小企業にとっては、これは非常に大切な点です。

22.Emily Maltby：「Chargebacks Create Business Headaches」、ウォール・ストリート・ジャーナル、2011年2月10日http://online.wsj.com/article/SB10001424052748704698004576104554234202010.html

しかし、消費者からは、悪徳業者や企業側のミスから保護されるので、支払拒否は歓迎されます。クレジットカードの業者アカウント料金のおかげで、消費者が他にも恩恵を享受できます。実際、ビットコイン決済が利用可能になっても、消費者や企業は伝統的なクレジットカードサービスを使い続けるでしょう。それでも、決済方法の選択肢が広がることで、いろいろな事情を抱えた人々

にくまなく恩恵が行き渡ります。

クレジットカードを通じた特典や消費者保護が必要な人は、多少余計に支払ってもカードを使い続けるでしょう。値段やプライバシーのほうを気にかける人々は、代わりにビットコインを利用できます。業者アカウントの手数料を支払わなくてもよいため、ビットコインを受け付ける企業は浮いた費用を消費者に還元することもできます。Bitcoin Store[23]はこのビジネスモデルを採用しており、ビットコインのみを受け付ける代わりに数千もの家電製品を割引価格で販売しています。Amazon.comでは779ドル＋送料[24]で売られているサムソンのギャラクシーノートタブレットがBitcoin Storeではたったの480ドルです。[25]こういうわけで、ビットコインは伝統的なクレジットカードサービス（こちらを好む消費者もいます）に煩わされず、出費を押さえたい消費者や中小企業に対して、より低コストなやり方を提供できます。

23.Vitalik Buterin：「Bitcoin Store Opens:All Your Electronics Cheaper with Bitcoins」ビットコインマガジン、2012年11月5日http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/
24.Amazon.comに掲載されたサムソンのギャラクシーノートタブレット、2013年5月29日にアクセスhttp://amzn.com/B00BJXNGIK
25.Bitcoinstore.comに掲載されたサムソンのギャラクシーノートタブレット、2013年5月29日にアクセスhttps://www.bitcoinstore.com/samsung-galaxy-note-gt-n8013-10-1-32-gb-tablet-wi-fi-1-40-ghz-deep-gray.html
ビットコインストア上の商品はビットコインとアメリカドルの両方で価格表示されています。購入時点では、ビットコインの決済サービス会社であるBitpayは通貨の両替レートを決定して価格を15分間維持していました。Bitcoinstore.comのFAQコーナーを参照してください。https://www.bitcoinstore.com/faq

安価な送金システムとして、ビットコインはローコストな送金サービスの未来に大きな可能性を提示しています。2012年度、先進国の移民が後進国に住む親類に当てて送金した額は最低でも4010億ドルに上りました。[26]送金額は、2015年までに5150億ドルに増加すると見込まれています。[27]これら送金のほとんどはウェスタンユニオンやマネーグラムなどの従来型の振込みサービスを通じて行われました。これらサービスには多額の手数料がかかり、送金が完了するまでに数営業日かかります。[28]2013年の第一四半期には、送金手数料の国際平均は9.05%でした。[29] 対照的に、ビットコインネットワーク内の取引手数料は0.0005BTC[30]（または取引総額の1%）以下にたいていは収まります。[31]起業家が送金環境を改善できるチャンスが生まれ、著名なベンチャーキャピタリストから投資を引き寄せています。[32]マネーグラムとウェスタンユニオンですら、ビットコインをビジネスモデルに取り込むことを検討しています。[33]ビットコインは送金を瞬時に、安価に行うことができ、消費者が享受できる国際送金のコスト減はかなりの規模になります。

26.World Bank Payment Systems Development Group：「Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services (Washington, DC: World Bank, 2013)」http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf
27.前記の箇所を参照してください。
28.Jessica Silver-Greenberg：「New Rules for Money Transfers, but Few Limits」ニューヨーク・タイムズ、2012年6月1日http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?pagewanted=all&_r=0
29.世界銀行による送金手数料
30.ビットコインウィキの見出し：「Transaction fees」、2013年7月30日にアクセスhttps://en.bitcoin.it/wiki/Transaction_fees
31.Andrew Paul：「Is Bitcoin the Next Generation of Online Payments?」 Yahoo!スモールビジネスアドバイザー、2013年5月24日http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--fi

nance.html
32.Simonite：「Bitcoin Hits the Big Time」
33.Andrew R. Johnson：「Money Transfers in Bitcoins? Western Union, MoneyGram Weigh the Option」ウォール・ストリート・ジャーナル、2013年4月18日http://online.wsj.com/article/SB10001424127887324493704578431000719258048.html

貧困と抑圧に対抗できる可能性

ビットコインは世界で最も貧困にあえぐ層の生活を手助けできる可能性を秘めています。基本的な金融サービスを利用しやすくすることで、効果的に貧困撲滅を推進できると期待されています。[34] ある試算によると、発展途上国に住む人々の64%が基本的な金融サービスを利用できていません。恐らくは、従来の金融機関にとっては貧乏な未開発地域にサービスを提供するのは割りに合わないのでしょう。[35]従来の銀行支店を貧困地域に配置するには障壁が大きいため、発展途上国の人々は金融ニーズを満たすためにモバイル銀行サービスを利用しています。閉鎖型モバイル決済サービスであるM-Pesaはケニヤ、タンザニア、アフガニスタンといった国々で特に大きな成功を収めています。[36] 起業家達は既にそのモデルに移行し始めています。ビットコインのオンライン財布サービスであるKipochiは最近、M-Pasaのユーザーがビットコインを両替できるようにするツールを開発しました。
[37] 発展途上国のモバイル銀行サービスはビットコインを採用すればさらに強化されます。オープンな決済サービスであるビットコインは発展途上国の人々に対して、グローバルな範囲で安価に金融サービスを利用する方法を提供できます。

34.Muhammad Yunus：「Banker to the Poor:Micro-lending and the Battle against World Poverty (New York: Public Affairs, 2003)」

35.Oya Pinar Ardic、Maximilien Heimann、Nataliya Mylenko：「Access to Financial Services and the Financial Inclusion Agenda around the World」（Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011）」https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf
36.Jeff Fong：「How Bitcoin Could Help the World's Poorest People」Policymic.com、2013年5月http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people
37.Emily Spaven：「Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa」Coindesk.com、2013年7月19日http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/

ビットコインはまた、資金規制が厳しい国に住む人々に逃げ道を提供することも可能でしょう。採掘可能なビットコインの数には上限があり、都合に合わせて操作することはできません。取引を拒否したり、国境を越えたビットコインの交換を禁止できる当局も存在しません。それゆえ、自国の価値が目減りした通貨や凍結した資本市場に代わるものを求めている人々にとって、ビットコインは脱出口となります。
資本規制や中央銀行の失策による負の影響から逃れるため、ビットコインに注目する人々の例が出現し始めています。例えば、アルゼンチン人の中には、25%のインフレ率と厳しい資本規制の二重苦のため、ビットコインを採用した人々もいます。[38]ビットコインに対する需要がアルゼンチンではあまりに大きいため、ある有名なビットコイン両替サービスはアルゼンチンに事務所を開設することを計画しています。[39] アルゼンチンの資本管理政策が失敗しているせいで、ビットコインを使うアルゼンチン人は増え続けています。[40]

38.Jon Matonis：｛Bitcoin's Promise in Argentina」フォーブス、2013年4月27日http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/
39.Camila Russo：「Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit」ブルームバーグ、2013年4月16日http://www.bloomberg.com/n

ews/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html
40.Georgia Wells：「Bitcoin Downloads Surge in Argentina」ウォール・ストリート・ジャーナル、2013年7月17日http://blogs.wsj.com/moneybeat/2013/07/17/bitcoin-downloads-surge-in-argentina/

抑圧されたり、非常事態のさなかにいる個人もまた、ビットコインが提供する金融的なプライバシー保護の恩恵を受けられます。金融取引においてプライバシー保護が求められるのには、納得できる理由がたくさんあります。暴力的な配偶者から逃れる人々には、追跡されることなくお金を使える方法が必要です。
賛否両論の治療法を試そうとする人々は、家族や同僚など、賛成を得られない人々には知られない金融サービスを利用したいと希望するでしょう。独裁国家の近年の歴史からわかるのは、独裁者の手を逃れて個人的に取引を行える方法があると、抑圧された市民にとって大きな助けになるということです。ビットコインはこれまで現金が担ってきたプライバシー保護機能をある程度まで提供できます。デジタル送金の便利さも付属してきます。

金融イノベーションの促進

ビットコインで最も期待される応用分野の一つは金融イノベーションのプラットフォームです。ビットコインプロトコルはプログラマーが簡単に便利な金融サービスや法律サービスを開発できるよう、デジタル的に仕掛けが内蔵されています。ビットコインの核を成すのは単純に言ってデータパケットのみなので、通貨だけでなく株式や投機、その他の機密情報を転送する用途にも使用できます。[41] マイクロ決済や争いの調停、契約の締結、あるいはスマート資産などの機能は、ビットコインプロトコルに既に組み込まれています。[42]これら機能を使用して、インターネッ

ト翻訳サービス、小額取引の即時決済（Wi-Fi利用状況の自動計量など）、Kickstarterのようなクラウドファンディングサービスを簡単に構築できます。

41.Jerry Brito：「The Top 3 Things I Learned at the Bitcoin Conference」Reason.com、2013年5月20日http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi
42.Mike Hearn：「Bitcoin 2012 London: Mike Hearn」 YouTubeビデオ、28:19、「QueuePolitely」により投稿、2012年9月27日http://www.youtube.com/watch?v=mD4L7xDNCmA
スマート資産はビットコインのブロックチェーン内の取引から生まれたアイテムの所有権を管理する試みです。スマート資産を利用すると、暗号法を通じて条件が一致すれば、モノやサービスの所有権を交換できます。スマート資産はまだ理論段階ですが、基本となる仕組みはビットコインのプロトコルに埋め込まれています。ビットコインウィキの見出し：「Smart Property」、2013年7月30日にアクセスhttps://en.bitcoin.it/wiki/Smart_Property

さらに、ウェブとメールがインターネットのTCP/IPプロトコルの上に構築されているように、プログラマーはビットコインのプロトコル上に別のプロトコルを構築することもできます。ネットワークの安定性とセキュリティを向上させるため、ビットコインのプロトコル上に新しいプロトコルレイヤーを構築することを提案したプログラマーもいます。[43]別のプログラマーは、ビットコインプロトコル上にデジタル公証サービスを作り上げ、匿名で安全に機密文書の「存在証明」を保管できるようにしました。[44] メール連絡を暗号化するためにビットコインモデルを採用したプログラマー達もいます。[45]ネットワークのプライバシー保護を改善できる追加プロトコルの原案を作成した開発者グループもあります。[46]ビットコインはこのように、他の機能レイヤーをその上に構築できるプラットフォームともなりえます。ビットコインプロジェクトは、金融やコミュニケーション上の実験プロセスと理解するのがもっともよいかもしれません。政治家は指導を行う際に、この未成熟なプロトコルの内部やその上で大

きな可能性を秘めたイノベーションが行われるのを阻害しないよう、注意する必要があります。

43.J. R. Willet：「The Second Bitcoin Whitepaper」白書、2013年https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf
44.Jeremy Kirk：「Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?」コンピューターワールド、2013年5月23日http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_notary_service_
45.Jonathan Warren：「Bitmessage:A Peer-to-Peer Message Authentication and Delivery System」ホワイトペーパー、2012年11月27日https://bitmessage.org/bitmessage.pdf
46.Ian Miersその他：「Zerocoin: Anonymous Distributed E-Cash from Bitcoin」調査結果報告書、ジョンズ・ホプキンズ大学コンピューターサイエンス部、バルティモア州、2013年http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

課題

ビットコインは数々の利点を持っていますが、これから使用を考えているユーザーが気をつけなければいけない点もいくつかあります。まず、誕生以来、ビットコインの価格は大きく変動してきました。新規ユーザーは、気をつけないとビットコインを不正に入手したり、誤って削除したりする危険性があります。さらに、ハッキングによりビットコイン経済が損害を被る懸念もあります。

変動性

2011年以来、ビットコインの大きな価格調整は少なくとも5回発生しています。[47]これらの調整は、昔からある投機的なバブルに似ています。メディアが過度に楽観的な口調でビットコインを取り上げ、新米投資家達が押し寄せてビットコインの値段を

押し上げるのです。[48]過熱はある時点で転換点を迎え、ビットコインの価値は下がり始めます。焦って参加する新米投資家はビットコインを過大評価する恐れがあり、下落と共にお金を失います。ビットコインの価値が変動するせいで、ビットコインの将来を疑問視する識者も大勢います。

47.Timothy B. Lee：「An Illustrated History of Bitcoin Crashes」フォーブス、2013年4月11日http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/
48.Felix Salmon：「The Bitcoin Bubble and the Future of Currency」Medium.com、2013年4月3日https://medium.com/money-banking/2b5ef79482cb

この変動性は、ビットコインの終わりを予言しているのでしょうか？そう信じる識者もいます。[49]変動性はビットコインの柔軟性を鍛える役割を持っており、変動性を打ち消す機能が開発されるにつれ、変動回数も減っていくだろう、と予測する人々もいます。[50] ビットコインが価値やアカウントを保存する目的のみで利用されるのであれば、変動性は確かにビットコインの将来を脅かすでしょう。予測不可能なやり方で市場価値が変動するのであれば、ビットコインで貯金したり、運用資金を活用する理由はありません。しかし、ビットコインを交換ツールとして使った場合は、変動性はそれほど問題になりません。[51]業者は商品に従来どおりの値付けを行い、同等のビットコインでの支払を受け付ければ済みます。客は、その場限りで買い物をするためにビットコインを購入するのであれば明日の為替レートがどう変化するかを気にすることはありません。ビットコインを使って、現時点の取引手数料を下げることにのみ興味があります。ビットコインの交換ツールとしての使いやすさを見れば、価格が変動するにも関わらず業者からの人気が増している理由がわかるでしょう。[52]より多くの人がビットコイン技術に慣れ、ビットコインの

将来に過大な期待を寄せなくなるにつれ、ビットコインの価値はそれほど変動しなくなるとも考えられます。

49.Maureen Farrell：「Strategist Predicts End of Bitcoin」CNNマネー、2013年5月14日http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html
50.Adam Gurri：「Bitcoins, Free Banking, and the Optional Clause」 Ümlaut、2013年5月6日http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/
51.Jerry Brito：「Why Bitcoin’s Valuation Really Doesn’t Matter」 Technology Liberation Front、2013年4月5日http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/
52.今日では、業者サービスは変動性のリスクを受け入れつつ、それでも手数料を低く維持しています。長期的にこのビジネスモデルが持続可能かどうかは、まだ不明です。

セキュリティ侵害

デジタル通貨として、ビットコインにはセキュリティ上の重要な課題がいくつかあります。[53]うっかりすると、ビットコインを誤って消去したり、別の場所へ移してしまうこともあります。デジタルファイルがなくなれば、紙幣と同様に、お金は失われます。各々が自分の所有するビットコインアドレスを守らなければ、盗んでくださいと言っているようなものでしょう。ビットコインのオンライン財布は暗号化で守られるようになりましたが、ユーザーは暗号化を手動で有効にしなければなりません。ユーザーが財布の暗号化を無効にしたままだと、悪意のあるソフトウェアに盗まれることになるでしょう。[54] ビットコインの両替サービスも、セキュリティ侵害に悩まされてきました。2012年にハッカー集団がビットコイン両替サービスのBitfloorから24000BTC（25万ドル）を盗み出し[55]、2013年には最も人気のあるビットコイン両替サービスのMt. Goxに大規模な分散型DDoS

（サービス妨害）攻撃をしかけています。[56]（Bitfloorはその後、盗まれた資金を顧客に払い戻し、Mt. Goxは最終的にDDoS攻撃から回復しました。）もちろん、ビットコインを巡るセキュリティリスクの多くは、従来の通貨が抱えるリスクに類似しています。ドル札は破棄したり失くしますし、個人情報は盗まれて犯罪者に利用されたりしますし、銀行は強盗にあったりDDoS攻撃に遭遇したりします。ビットコインのユーザーは、他の金融活動に対して既に行っているのと同様に、セキュリティ懸念について学び、準備しておく必要があります。

53.安全性の課題はほぼ全て、財布サービスとビットコインの両替に関わります。ビットコインのプロトコル自体は、ハッカー攻撃とセキュリティ上のリスクに対してかなりの耐性を発揮することが証明されています。著名なセキュリティ研究家であるDan Kaminskyは2011年にビットコインプロトコルをハッキングしようとして、失敗しました。Dan Kaminsky：「I Tried Hacking Bitcoin and I Failed」ビジネス・インサイダー、2013年4月12日http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4
54.Stephen Doherty：「All Your Bitcoins Are Ours . . . 」 Symantecブログ、2011年6月16日http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours
55.Devin Coldewey：「$250,000 Worth of Bitcoins Stolen in Net Heist」 NBCニュース、2012年9月5日http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871
56.Meghan Kelly：「Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month」 VentureBeat.com、2013年4月21日http://venturebeat.com/2013/04/21/mt-gox-ddos/

犯罪目的の利用

政治家がビットコインに寄せられる賞賛に対して危惧を抱くのも、理由があります。ビットコインは半匿名であるため、政治家やジャーナリストからは、犯罪者が資金洗浄や非合法な商品やサービスの決済にビットコインを使えるのではないか、と疑問が提示さ

れてきました。実際、現金と同じく、ビットコインはよい目的にも悪い目的にも使えます。

例えば、「シルクロード」と呼ばれる、深層ウェブ（一般的な検索エンジンでは情報収集できないウェブ）[57]上に存在する悪名高い闇市場のケースを見て見ましょう。シルクロードはネットワークを匿名化するTorとビットコインの半匿名性を利用して、麻薬やその他の合法・非合法な商品を通信販売できる広大なデジタル市場を利用可能にしました。
シルクロードの管理者達は盗難されたクレジットカード情報や幼児虐待の写真など、詐欺や悪意から生まれる商品の取引は禁じていますが、偽造した身分証明書や違法なドラッグなどの非合法商品の販売は許可しています。これまで現金を利用して個人間で違法な売買を行っていたのと同様に、買い手はビットコインの半匿名性を利用してオンラインで非合法な商品を購入できます。ある試算によると、シルクロードの月間合計取引額は約120万ドルに達します。[58]しかし、2013年7月度にビットコイン市場は7.7億ドルを記録しました。シルクロードの売り上げはビットコイン経済全体からすると雀の涙程度の大きさです。[59]

57.ウィキペディア、見出し：「Deep Web」2013年7月30日にアクセスhttp://en.wikipedia.org/wiki/Deep_Web
58.Nicolas Christin：「Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace」 カーネギーメロンCyLab技術レポート、CMU-CyLab-12-018、2012年7月30日（2012年11月28日に更新）http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf
59.Jerry Brito：「National Review Gets Bitcoin Very Wrong」 Technology Liberation Front、2013年6月20日http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/

シルクロードと関連付けられることで、ビットコインの評判に傷がついています。シルクロードに関する記事[60]が発表された

後、チャールズ・シュマー（Charles Schumer）とジョー・マンチン（Joe Manchin）上院議員は法務長官のエリック・ホルダー（Eric Holder）と麻薬取締局の長官であるミシェル・レオナート（Michele Leonhart）にシルクロードと匿名化ソフトのTor、それにビットコインの摘発を促す手紙を出しました。[61]

60.Adrian Chen：「The Underground Website Where You Can Buy Any Drug Imaginable」ギズモード、2011年6月1日http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable
61.Brett Wolf：「Senators Seek Crackdown on ‘Bitcoin’ Currency」ロイター、2011年6月8日http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608

もう一つの懸念は、テロ活動の資金提供や非合法商品の密売用として、資金洗浄が行われる過程でビットコインが使われる、というものです。この懸念は、現時点ではまだ事例があってというより理論的なものですが、ビットコインは不正に取得した資金を秘密裏に移動させたい人間にとっては、確かに手段の一つになりえます。ビットコインが資金洗浄に利用される可能性がある点への懸念は、コスタリカに拠点を置く私的な中央集権型のデジタル通貨サービスであるLiberty Reserveが資金洗浄の疑いで当局によって閉鎖されて以来、より高まっています。[62]

62.「Liberty Reserve Digital Money Service Forced Offline」 BBCニュース・テクノロジー、2013年5月27日http://www.bbc.co.uk/news/technology-22680297

Liberty Reserveとビットコインはどちらもデジタル通貨を提供するので、似たもの同士に思われますが、両者の間には重要な差異があります。Liberty Reserveは私企業によって創立され保有

されていた、中央集権型の通貨サービスでした。明らかに資金洗浄を助ける目的をもっていた、とされています。ビットコインはそうではありません。Liberty Reserve経済内では透明な取引は行われませんでした。実際、Liberty Reserveは顧客に匿名性を保証していたのです。一方でビットコインは権力分散型のオープンな通貨であり、全ての取引記録は公開されています。資金洗浄業者は自身のビットコインアドレスや身元を隠そうとするでしょうが、取引記録は常に公開され、当局はいつでも参照できます。ビットコインを通じた資金洗浄は、Liberty Reserveのような中央集権型のシステムを用いた場合よりもずっと危険な行為と言えます。さらに、数社のビットコイン両替サービスは資金洗浄防止に向けた記録保持と報告の要求に適合するため、自ら努力を行っています。[63] 公開台帳システムと合わせて、ビットコイン両替所が顧客情報を協力的に収集すれば、資金洗浄業者にとっては私的で匿名な仮想通貨に比べてビットコインの魅力は薄れていくはずです。

63.Jeffrey Sparshott：「Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules」ウォール・ストリート・ジャーナル、2013年6月28日http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html

また、考えられるビットコインの短所は、これまでの現金にまつわる短所と同じである、と認識しておくことも大切です。歴史的に、麻薬の運び人や資金洗浄業者にとって現金は主要な運用手段でした。しかし、政治家は現金を禁止しようと真剣に考えたことはありません。規制機関がビットコインを検討し始めた今、彼らは過剰な規制こそ気にかけるべきでしょう。最悪の事態とは、規制機関のおかげで合法なビジネスがビットコインネットワークの恩恵を受けることができず、その一方で資金洗浄業者や麻薬の運び人が自由にビットコインを扱える状態です。例えばビットコイ

ン両替所が規制に耐えかねて商売を畳んでも、資金洗浄業者や麻薬の運び人はビットコインを彼らのオンライン財布に送金してくれる個人に謝礼を払って、ネットワークに資金を入れることはできます。この場合、過剰な規制のせいで良質な取引が止められ、本来規制されるべき対象は活動を続けられます。政治家と規制機関の課題は、ビットコインによって合法的なユーザーが日常的に恩恵を受けられる状態を維持しつつ、資金洗浄と非合法な売買という二重の懸念を緩和できるシステムをいかに構築できるか、にあります。

規制

現在の法律と規制はビットコインのような技術を考慮しておらず、法的には未整備な状態にあります。この事態が起こっている大きな理由は、ビットコインが通貨や金融ツール・機関に関する既存の法的解釈にぴったりと収まらないため、どの法律をどうやって適用すればいいのかがわかりにくい、という点にあります。
この状況は、VoIP（IP電話）など他の新興技術にまつわる規制上の不確定さを思い起こさせます。[64]VoIPが最初出現した時、米国通信法とFCC（連邦通信委員会）は既存の公衆交換電話網で行われる音声通話のみを取り扱おうとしました。ビットコインのように、VoIPは高度に規制された既存の通信網と競合しており、より安く提供され、主にピアツーピアの性質を持っていました。今日に至るまで、連邦議会とFCCはVoIP政策について寄せられる疑問と格闘しています。VoIPのプロバイダーにはどの公益義務が課せられるのか、あるいはVoIPプロバイダーは警察による盗聴要請に従う必要があるのか、などです。

64.Sam Rozenfeld：「FCC’S VoIP Regulation Dilemma」 Telephony Your

Way、2011年4月30日http://www.telephonyyourway.com/2011/04/30/fccs-voip-regulation-dilemma/

幸いにも、連邦議会とFCCは規制上の不明瞭さのほとんどを明確にし、かつ独占的な電話サービスに対して設けられた従来の規制を新興技術に負担させないことで、VoIPに対して道を開いてくれました。結果として、VoIPは技術的に繁栄し、それまで硬直していた市場に競争原理を導入し、消費者にとってはより扱いやすく低コストになりました。政治家はビットコインについても同じことを行うべきです。

ビットコインは電子決済システム、通貨、商品などの属性を持っています。結果として、複数の規制機関から監査を受けるでしょう。こうした機関がビットコインの規制を始めようと準備するに当たって直面するであろう疑問を、以下に並べてみました。

私的通貨は合法なのか？

ビットコインに寄せられる初歩的な質問で最も多いものの一つが、連邦政府が独占的に法定通貨を発行できる事実を考慮した上で、オンライン貨幣が合法であるかどうか、です。答えは、どうやら「イエス」のようです。合衆国憲法によると、各州に禁止されているのは硬貨の鍛造のみです。[65]通貨の私的発行は禁止されておらず、実際多くの地域通貨が流通しています。[66]地域通貨を広めるために、経営者や議員は近年、代替通貨をいくつか作り上げてきました。オレゴン州ポートランドのCascadia Hour ExchangeやワシントンDC州ベーリンガムのLife Dollarsなどです。[67]

65.アメリカ合衆国憲法、条項I § 10

66.Reuben Grinberg：「Bitcoin: An Innovative Alternative Digital Currency」Hastingsサイエンス＆テクノロジー法律ジャーナル、2011年第四号、159-208ページ
67.Blake Ellis：「Local Currencies: 'In the U.S. We Don't Trust,'」 CNNマネー、2012年1月27日http://money.cnn.com/2012/01/17/pf/local_currency/index.htm

私的な組織が行うべきでないのは、ドルによく似た通貨を発行することです。[68]悪名高い例に、金建ての「Liberty Dollar」を印刷して発行し、2011年に起訴されたBernard von NotHausがあります。彼が犯した犯罪は代替通貨を発行したことではなく、通貨の外見が米ドルに似ており、彼が自身の通貨をドルに混ぜて流通しようとし、他人にもそれを推奨していたことです。[69]対照的に、ビットコインはドルと混同される恐れはありません。

68.18 アメリカ合衆国憲法、条項 § § 485 と 486
69.Grinberg：「Bitcoin」 193n158

送金法

個人間で資金を移動するビジネスは送金業に該当し、48州とコロンビア特別区（ワシントンD.C.）ではライセンス取得が義務付けられています。[70]送金業者はFinCENの規制を元に施行される銀行秘密法（BSA）の対象にもなります。さらに、米国愛国者法によって、未許可で送金ビジネスを行う者は刑事犯として扱われるようになりました。[71]

70.非銀行系の送金業者やマネーサービスビジネスへの規制に関する公聴会、第112回国会（2012年）（Ezra C. Levineによる証言）金融サービスに関する下院委員会内の金融機関と消費者信用に関する小委員会にてhttp://financialservices.house.gov/uploadedfiles/hhrg-112-ba15-wstate-elevine-20120621.pdf

71.18 アメリカ合衆国憲法 § 1960

州ごとに送金業のライセンスを発行していた理由は、これまでは消費者保護が目的でした。[72]送金業（郵便為替の発行業者など）は、大抵の場合FDIC（連邦預金保険会社）によって保証された銀行ではないので、送金業者が受取人に送金を行わなかった場合は、消費者が全責任を負っていました。ライセンス制は、この危険性を和らげるためにあります。送金業者が州ごとにライセンスを取得する方式が広まったのは、1980年代に郵便為替業者の債務不履行がいくつも発生し、それがよく知られるようになってからです。[73]

72.Aaron Greenspan：「Held Hostage: How the Banking Sector Has Distorted Financial Regulation and Destroyed Technological Progress (Palo Alto, CA: Think Computer Corporation, 2011)」http://www.thinkcomputer.com/corporate/whitepapers/heldhostage.pdf
73.前記の箇所を参照してください、3

一方でBSAは、資金洗浄とテロ資金提供を防ぐことが目的です。[74]送金業者や他の金融機関はFinCENに登録し、資金洗浄防止策を実行し、顧客情報の記録を取り、疑いのある取引や他のデータを報告する必要があります。ビットコインは企業でも法的組織でもなく、グローバルなピアツーピアネットワークであるため、それ自身は送金業者とは言えません。となると疑問は、ビットコインの生態系内で「送金業者」の法的定義に合致し、州法と連邦法の管轄の対象となる要素はあるのだろうか？ということになります。

74.31 アメリカ合衆国憲法 § 5311

2013年3月、FinCENはBSAをビットコインを含めた仮想通貨に適用するためのガイドラインを発行しました。ガイドラインに

は、送金業者の規制対象になりうる三種類の人々が定義されています。

> ユーザーとは、仮想通貨を所持してモノやサービスを購入する個人を指します。両替人は仮想通貨を実効通貨、資金、または他の仮想通貨に両替するビジネスに携わる個人を指します。
> 管理者は仮想通貨を発行（流通に乗せる）ビジネスに携わる個人を指し、そのような仮想通貨を換金（流通から外す）する権限を持っています。[75]

75.FinCEN：「Application of FinCEN’s Regulations」

各定義は、ビットコイン生態系内の人々に適用が可能です。最も明確な定義は、両替人です。ドルとビットコインに両替、またはその逆を行う個人は、このガイドラインによると送金者であると結論できます。FinCENに登録し、関連する記録保持や報告の義務に従う必要があります。また、各州はどの組織が送金業者に該当するのかをFinCENの決定を参照することが多いので、両替人は州により発行された送金業者ライセンスを取得しなければならない可能性が高くなります。

あまり直感的にわかりやすくないのは、ただのビットコイン「ユーザー」が守らなければならない義務です。ガイドラインによると、「仮想のモノあるいはサービスを購入するため」にビットコインを所持する個人は送金者ではなく、FinCEN規制の対象にはなりません。しかし、モノやサービスを購入する目的以外でビットコインを所持する個人に対して法律がどう適用されるのかは、説明されていません。ビットコインを購入以外の目的で所持する理由としては、以下があります。（1）ビットコイン価格が上昇

するという思惑、（２）単に、特定の「実効通貨」（例えばアルゼンチンやジンバブエ）よりも仮想通貨のほうを信頼しているため、（３）外国に住む家族に送金したいため上記のいずれの例においても、ビットコインユーザーはFinCENの規制や、記録保持と報告の義務から、解放されるという保証はありません。不明瞭な規制環境が生まれることになり、ビットコインの使用を過度に控えることにつながりかねません。

最もわかりにくのは、ガイドラインがビットコインの採掘者に対してどう適用されるか、という点です。採掘者はビットコインネットワークにコンピューター処理能力を貢献して、新たなビットコインを作成する人々です。ガイドランが定義する第三のカテゴリは「管理者」です。しかし、この定義は中央に位置する権威が通貨を発行する中央集権型の仮想通貨にのみ当てはまります。例えば、Amazon.comは明らかに、自身の仮想通貨、「アマゾンコイン」の管理者です。[76]ガイドラインはそれゆえ、ビットコインのように権力分散型の仮想通貨を取り扱った章を設けています。その章によると、ビットコインを採掘して「実体のある、または実体のないモノやサービスを購入するため」にそれを使う採掘者はユーザーに該当し、規制対象にはなりません。[77] しかし、採掘者が採掘済ビットコインを「他者に対して、実効通貨またはその代替と引き換えに」売る場合、採掘者は送金者として規制の対象になります。[78]

76.Ingrid Lunden：「Amazon Now Offers Amazon Coins Virtual Currency on Kindle Fire, Gives $5 in Free Coins to All Users」 TechCrunch、2013年5月13日http://techcrunch.com/2013/05/13/amazon-launches-amazon-coins-virtual-currency-on-kindle-fire-gives-5-in-free-coins-to-all-users/
77.前記の箇所を参照してください。
78.前記の箇所を参照してください。

そのような送金者としての採掘者に対する規制が消費者の保護や資金洗浄防止を促進するかどうかは、不明です。採掘者はビットコインを関係者の間で移動させているわけではありません。彼らは何もないところからビットコインを生み出しているのです。採掘者が、自身が採掘したビットコインを販売する場合、そこには彼らと買い手の二者しか存在しません。結果として、保護するべき消費者も、「汚れた資金」をクリーンな資金に変換しようとする犯罪者も存在しません。

最後に、FinCEN規制が通貨を州によって発行される通貨と定義するように、ガイドラインで言う「実効通貨」もその定義に従う、とガイドランには記載されています。[79]続いて、ガイドラインの全てで前提となる「仮想通貨」という新しい概念を策定しています。[80]ガイドラインによると、仮想通貨は「実効通貨のように交換媒体として機能する環境もあるが、実効通貨が持つ属性を全て備えているわけではない」と定義されています。[81]続いてガイドラインは新たな概念を提唱し、「仮想通貨」は各種あり、現行のガイドラインは「実効通貨においても同等な価値を保つか、実効通貨の代替として機能する」と定義される「両替可能な仮想通貨」のみに適用されるとしています。[82]通貨（つまり、「実効通貨」）の定義はルール作成の過程を経て採択されましたが、「仮想通貨」と「両替可能な仮想通貨」という新しくて実質的な概念はガイドライン内にのみ存在します。その結果、ガイドラインは既存の法律や規制を単に解釈したものではなく、新たな法律を包含している、と理解される可能性があり、それゆえに行政手続法に従ったルール作成が必要になってきます。

79.FinCEN：「Application of FinCEN’s Regulations」
80.前記の箇所を参照してください。
81.前記の箇所を参照してください。

82.前記の箇所を参照してください。

CFTC規制

ビットコインはその性質上、通貨としても商品としてもみなせます。実際、経済学者のジョージ・セルギン（George Selgin）はビットコインを「商品合成通貨」と呼びました。[83]これが商品先物とその取引市場や外国為替手段を規制する商品先物取引委員会（CFTC）の目に留まりました。CFTCは商品先物とその市場を規制する権限を持ち、いくつかの外国為替手段も規制しています。[84]

83.George Selgin：「Synthetic Commodity Money” (working paper, Department of Economics, University of Georgia, Athens, 2013)」http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118
84.7 アメリカ合衆国憲法、条項 § § 2(C) と 2(E)

CFTCの五人の理事の一人、バート・チルトン（Bart Chilton）は最近、フィナンシャル・タイムズ紙に対してビットコインは「間違いなく研究が必要だ」と語りました。[85]他の情報筋からも、CFTCは「真剣に」仮想通貨を調べ始めていると伝わってきます。[86]CFTCがビットコイン取引を規制すると決定したとして、自明な疑問の一つは、規制の管轄が商品先物になるのか、外国為替になるのか、です。

85.Alloway、Meyer、Foley：「US Regulators Eye Bitcoin」
86.前記の箇所を参照してください。

商品取引法では「為替予約取引」と「為替スワップ取引」は定義されていますが、「外国為替」と「外国通貨」は定義されていま

せん。恐らくは、国会でこれらの用語は意味が明白だ、とされたのでしょう。ゆえに、もしCFTCが外国為替規制をビットコイン取引に適用しようとした場合、ビットコインは「外国通貨」と考えられる、と決定する必要があります。そのような決定はあり得る話ですが、そうなると外国政府によって鍛造される通貨、という外国通貨の一般的な定義が当てはまりません。

もっと具体的にとらえるために、CFTCが外国為替を規制する権限を拡大した、2009年のドッド・フランク・ウォールストリート改革および消費者保護法を見てみましょう。法律の第十章では消費者金融保護局（CFPB）が規定され、その目的の一環として「外国為替」は「アメリカ合衆国または外国政府の通貨を、支払のために別の国の通貨と交換する行為」と定義されています。[87] この定義を通じて、議会が考える「外国為替」とは何か、のヒントが得られます。ビットコインはどの国の通貨にも属さないので、明らかにその定義から外れています。

87.ドッド・フランク法、ドッド・フランク・ウォールストリート改革および消費者保護法 § 1002 (16); 12 アメリカ合衆国憲法 § 5481 (16) (2012)

外国通貨は政府により発行される、と普通に理解されています。財務省では、通貨は次のように定義されます（前記のとおり、ルール作成の過程を経て採択されたものです）：

> アメリカ合衆国または他のあらゆる国の、紙幣や硬貨の形をとった金銭であり、法定通貨だとみなされて流通しており、発行元の国では交換用の媒体として日常的に使用され受け入れられているもの。通貨には、米国銀証券、米国紙幣、連邦準備券が含まれます。通貨にはまた、交換手段として外国で一般に使用されている、正式な外国の紙幣も含

まれます。[88]

88.31 CFR（連邦規制基準） § 1010.100(m) を参照してください。

これは統一商事法典でいう「金銭」の定義に適合します。「国内または外国政府により承認もしくは採用された交換手段であり、政府間の組織または二カ国以上の合意によって設立された口座内の通貨単位を含む」[89]

89.統一商事法典§§ 1-201

対照的に、CFTCはビットコインを商品として扱うことに問題はないでしょう。商品先物法では、商品とは全ての「将来的に引渡しされることが現在または将来の契約に盛り込まれているモノや条項…そして全てのサービス、権利、利益」（玉ねぎと映画の興行収入を除いて）と定義されています。[90]ゆえに、ビットコインは取引が可能な条項であり、先物契約の対象となるため、確かに商品に該当します。しかしながら、形のある実体を持ち、それ自体に使い道のある金やコーン、石油といった従来の商品とは、ビットコインは異なるという点は注意しておいたほうがよいでしょう。また、CFTCの管轄権限は商品そのものではなく、商品先物であることも覚えておくことは重要です。ビットコインとドルや他の外国通貨の交換は、通常一瞬で終了するため、先物取引とはみなされません。それゆえ、ビットコインを商品としてみなした場合のCFTCの規制は限定されたものになるでしょう。しかし、ビットコインの将来市場の発展に限って言えば、確実にCFTCの管轄に入ります。[91]

90.7 アメリカ合衆国憲法 §1a (9)
91.しかし、ビットコイン先物市場も発展しつつあります。Cyrus Farivar：「‘Taming the Bubble’：Investors Bet on Bitcoin via Derivatives Markets」 Ars T

echnica、2013年4月11日http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/

電子資金取引規制

既存の法規の元でビットコインにかけられる可能性のある規制について、最後に我々が注目するのは電子資金取引法（EFTA）[92] と連邦規制条項Eを通じて施行される法律の適用です。[93]EFTAの目的は金融機関や消費者が電子資金取引を行う上での権利や責任を打ち出すことです。[94]これまで取り上げてきたほかの法律や規制と同様に、EFTAはビットコインのような権力分散型の仮想通貨を想定していないようです。

92.15 アメリカ合衆国憲法、条項 §§ 1601-1692 (2013)
93.12 CFR（連邦規制基準） § 205.1-205.20 を参照してください。
94.15 アメリカ合衆国憲法 § 1693(b)

法律によれば、電子資金取引とは次のように定義されます。「金融機関に対して口座に振込みや引き落としを行う命令、指示、または許可を行うために、電子端末、電話機器、またはコンピューターや磁気テープを通じて行うあらゆる資金転送（小切手、為替手形、または同様な書類を用いたものを除く）」[95]さらに、法律では「金融機関」をこう定義もしています。「州立または連邦銀行、州立または連邦の貯蓄貸付組合、相互貯蓄銀行、州立または連邦信用組合、または消費者に属する口座を直接的または間接的に所有するあらゆる個人」[96] これらの定義と、それらが補強する規制は、電子的な資金の移動は「金融機関」と「口座」が伴うはずだ、と前提を行っています。しかし、ビットコインはその考えと矛盾します。

95.15 アメリカ合衆国憲法 §1693a (7)
96.15 アメリカ合衆国憲法 §1693a (9)

ビットコインシステム自体は、以前にも記述したように企業や法的組織ではなく、グローバルなピアツーピアネットワークであるため、「金融機関」には該当しません。結果として、ネットワーク上でビットコインが関連付けられているビットコインアドレスは金融機関内の口座とは言えません。さらに、ビットコインがアドレス間で転送される技術的な仕組みでも書いたように、ビットコインシステム内には「口座に振り込んだり、口座から引き落としたりする」金融機関や他の第三者は存在しません。アドレス間の電子的な資金の移動は、自身が管理するビットコインアドレスに結び付けられた秘密鍵を用いて取引に署名するユーザーのみが行います。ビットコインネットワークは、単に取引が正式であることを検証するだけです。

多くのユーザーは自身のコンピューターや他のデバイス内[98]に「財布ファイル」[97]を持ち、秘密鍵をそこにいれています。オンラインの財布サービスに鍵を預け入れるユーザーもいます。[99]そうしたサードパーティーの財布サービスでは、ビットコインのデスクトップソフトよりもはるかに使い勝手がよくなることが多いのです。そのような財布サービスでは、ユーザーは通常「アカウント」を作成し、自身のビットコインアドレスがアカウントに結び付けられます。そうしたオンラインサービスはEFTAで定義された「金融機関」に該当し、ゆえに規制の対象とされる可能性はあります。しかし、こうしたサービス自体は送金を行わないため、電子的な送金サービスに携わっているわけではない、という主張は可能です。[100]転送はユーザーが直接行い、ビットコインネットワークにより認証されます。オンラインの財布サービスは単に、ユーザーがビットコインネットワークを扱える

ようにソフトウェアと保管場所を提供しているだけに過ぎません。

97.ビットコイン　ウィキ、見出し：「Wallet」2013年7月30日にアクセスhttps://en.bitcoin.it/wiki/Wallet
98.Matthew Sparks：「Winklevoss Twins Back Bitcoin as Bubble Bursts」テレグラフ、2013年4月12日http://www.telegraph.co.uk/technology/news/9989610/Winklevoss-twins-back-bitcoin-as-bubble-bursts.html
99.ビットコイン　ウィキ、見出し：「EWallet」2013年7月30日にアクセスhttps://en.bitcoin.it/wiki/EWallet
100.Nikolei M. Kaplanov：「Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation」 Loyola消費者法レビュー、25、2012年第一号

最後に、消費者金融保護局（CFPB）が規制Eを改正した新ルールは、為替送金業者を対象にしています。送金業者は国際送金に関する両替レートと手数料を公開し、手続エラーが発生した際には調査を行って修正をかける必要があります。[101]消費者には30分以上の送金キャンセル期間を与えることも義務付けられています。[102]ビットコインの取引は全て非可逆なので、この要求はビットコインのプロトコルと相容れないと考えられます。この規制に適合する方法の一つは、取引の実行を遅らせることです。しかしそれよりも、真の問題は、この要求がビットコイン技術の目的と根本的に衝突することです。

101.消費者金融保護局：「Summary of the Final Remittance Transfer Rule (Amendment to Regulation E)” (Washington, DC: Consumer Financial Protection Bureau, 2013)」http://files.consumerfinance.gov/f/201305_cfpb_remittance-transfer-rule_summary.pdf
102.前記の箇所を参照してください。

政策提言

これまで見てきたように、ビットコインは既存の規制範囲にはう

まく収まりません。革新的な技術は、しばしそうした特長を持ちます。まさに、ビットコインは人類の繁栄に大きな恩恵をもたらす可能性を持つ、革新的な技術成果です。しかし、善い目的に使える技術全てと同様に、悪用することも可能です。政治家の課題は、ビットコインの負の影響を最小化しながら長所を育てることです。この課題を達成できるよう、政治家に対していくつか提言を行うことで本書を締めくくろうと思います。

ビットコインを制限してはならない

ビットコインは本質的にオンライン上の現金であり、麻薬や他の非合法な商品をオンラインで扱う人々の中には、理想的な交換手段として目をつけている者もいます。[103]こうした事実を目の当たりにすると、政治家の中には技術を制限しよう、ととっさに反応する人々もいます。[104]しかし、そうした衝動を抑えたほうがよい理由がたくさんあります。

103.Andy Greenberg：「Founder of Drug Site Silk Road Says Bitcoin Booms and Busts Won’t Kill His Black Market」フォーブス、2013年4月16日http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/
104.Charles Schumer、Joe Manchin著：司法長官Eric Holderと麻薬取締局長Michele Leonhartに対する手紙、2011年6月6日、以下にて閲覧可能：http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3

まず、一介の技術として、ビットコインは善くも悪くもありません。中立です。ドル札も、ビットコインのように非合法な取引に使えますが、紙幣を非合法化しようと考える者はいません。単に、非合法な使用を禁じるだけです。さらに、ビットコインの犯罪取引での使用は事例証拠しかありません。技術の犯罪利用は、合法

的な利用と比較しながら扱うほうが賢いやり方でしょう。ドル札と同様に、ビットコイン経済が発展するにつれ、合法的なビットコイン利用が犯罪取引を圧倒していく[105]のが予想されます。

105.Jan Jahosky：「BitPay Eclipses Silk Road in Bitcoin Sales with Explosive $5.2M March」 BitPayブログ、2013年4月2日http://blog.bitpay.com/2013/04/bitpay-eclipses-silk-road-in-bitcoin.html

第二に、ビットコイン技術を制限しようとすると、どう試みても合法的な利用を損なうだけにとどまり、非合法な利用はあまり影響を受けないでしょう。ビットコインは権力分散型のグローバルネットワークであるため、閉鎖することは現実的に不可能です。目標にできるビットコイン企業やその他の組織は存在しません。代わりに、ビットコインとその台帳はユーザーが作り出したピアツーピアネットワークに分散して存在するだけです。ピアツーピアのファイル共有サービスであるBitTorrentと同様に、ピアツーピアを構成するコンピューターを個別に閉鎖しても、ネットワーク全体にはほとんど影響がありません。ゆえに、ビットコインを非合法にしてもネットワークの活動は消えません。法を重んじるユーザーが技術を扱えなくなるようにするだけで終わります。結果として、犯罪利用は少しも減らないにも関わらず、ビットコインの利点の多くは社会で利用できなくなります。

第三に、もしビットコインが禁止されたら、政府は両替人や送金業者といったビットコイン経済内の仲介業者を規制する機会を失います。政府が資金洗浄とテロ資金提供を摘発して防止する活動を広げるには、技術を禁止するよりも、従来の金融機関と同様に仲介業者に対して記録を残して疑わしい活動を報告するよう義務付けるほうがよいでしょう。繰り返しますが、ビットコインを使うことを禁止しても犯罪者だけがその技術を使うことになるのは確実です。両替商や決済サービスなどで、不法な仲介業者が発生

しても、それらが取り締まられることはありません。

最後に、アメリカ合衆国がビットコインの使用を禁止しても、他の国々はビットコインが持つたくさんの長所を認め、使い続ける可能性が高いでしょう。例えば、フィンランド中央銀行がデジタル通貨は非合法ではない[106] と宣言したために、多くのフィンランド企業がビットコインを受け付け始めました。[107] ビットコインの使用を禁止すると、アメリカ合衆国は次世代の決済システムになりうるものを利用し発展させる上で、国際的に不利な立場に自らを置くことになります。

106.Matt Clinch：「Bitcoin Utopia? Interest Is Sky High in This Euro Nation」CNBC、2013年4月4日http://www.cnbc.com/id/100618694
107.Jan Jahosky：「BitPay Exceeds 1,000 Merchants Accepting Bitcoin」BitPayブログ、2012年9月11日http://blog.bitpay.com/2012/09/bitpay-exceeds-1000-merchants-accepting.html

規制を標準化してさらなる発展を促せ

ビットコインの不法利用に過剰反応するより、政治家は新規技術がもたらす課題には慎重で落ち着いた対応を行ったほうが得策でしょう。そうすれば、警察組織も資金洗浄とテロ資金提供活動の摘発と防止を推進しつつも、社会でビットコインが持つ多くの長所が利用されることを邪魔せずにすむでしょう。幸いにも、規制機関は今日に至るまでビットコインを既存の金融規制の枠組みに少しずつ組み込むことで、慎重な対応をとってきました。政治家は基本的な手法をいくつか押さえておけば、バランスを確保できます。

短期的には、FinCENは最近発行したガイドラインをより明確に

する必要があります。特に、モノやサービスの購入用ではなく他の合法で正当な目的のためにビットコインを所持する採掘者やユーザーを対象としているからです。告知と意見収集のプロセスを正式に公開して、開発者、採掘者、企業、ユーザーから成るビットコインコミュニティが公に参加できるようにすることで、それが可能になります。
FinCENの使命は金融システムを不法利用から守ることであるのは確かですが、同時に技術革新を過度に妨げることもしない義務を負っています。ビットコインの合法的なユーザーと協力すれば、FinCENは間違いなく規制上の不明瞭さを最小限に抑えつつ使命を達成できるでしょう。

長期的には、政治家はビットコインの規制上の立場をもっと広範囲に定義する必要があります。これまで見てきたように、デジタル通貨がぴったりと収まる既存の仕分けや法律上の定義は存在しません。
ビットコインは外国通貨でもなく、従来の商品でもなく、さらには単なる決済ネットワークでもありません。従って、既存のルールをビットコインに適用すると、警察組織や消費者にとっての利益を付随することなく、ビットコインが正当に発展することを過度に邪魔することになります。そういうわけで、政治家はビットコイン技術のユニークな性質を考慮して、新しいカテゴリの策定を検討するのがよいでしょう。ビットコインの両替商、決済サービス、ユーザーがどの規制の対象に入るか、慎重に検討する必要もあります。

最後に、政治家はビットコインが阻害されることなく発展を続けられるようにするだけではなく、既存の規制障壁を見直すことでもビットコインの発展を手助けするべきです。ビットコインが合法的に採用されるための最大の難関の一つは、送金に携わる企業

が各州からライセンスを取得する義務です。これは二度手間で、煩雑で、費用がかかる手続きであり、州を越えて取引を行う障壁になっており、その一方で消費者はほとんど恩恵を被ることはありません。連邦に属する政治家や規制機関は、専占（連邦法に矛盾する州法の無効化）を検討する必要があります。

結論

ビットコインは人々の生活に恩恵をもたらし、決済、コミュニケーション、ビジネス上に有利なだけでなく革新的な発展の可能性を秘めた、刺激的なイノベーションです。ビットコインは公開鍵暗号化とピアツーピアネットワークを巧妙に使用して、これまで権力分散型の通貨を阻んできた二重使用の問題を解決しました。こうした性質を組み合わせれば、ビジネスや送金の手数料を下げ、貧困を和らげ、資本支配や金融不正を逃れる手段を提供し、オンライン上で合法的に資産保護を行え、新たな金融イノベーションを引き起こせる決済システムが出来上がります。一方で、「デジタル通貨」としてビットコインは資金洗浄や不正取引にも使えます。ビットコインを禁止しても資金洗浄や不正取引を終わらせることにはなりません。現金を禁止しても、そうした問題の解決にならないのと同じです。

ビットコインは、実験的なデジタル通貨と決済システムとして、最終的には失敗に終わる可能性もあります。予期しない問題が起こり、ビットコイン経済を破滅させるかもしれません。もっと優れた暗号化通貨がビットコインを駆逐し、置き換えるかもしれません。一過性の流行として、単に消えていく可能性もあります。失敗する可能性は無限にありますが、政治家が仕組みと可能性を理解できなかった、は失敗の理由になってはいけません。なぜな

ら、私達は究極的にはビットコインを支持しているわけではなく、イノベーションを支持しているからです。政治家がこの実験を存続させることは重要です。政治家はビットコインがどう規制されるかを明確にし、規制を標準化することで人々がビットコインの革新性を学べる機会を提供できるよう、努力する必要があります。

参考資料

Satoshi Nakamoto「Bitcoin: A Peer-to-Peer Electronic Cash System」 白書、2008年http://bitcoin.org/bitcoin.pdf.

Reuben Grinberg 「Bitcoin: An Innovative Alternative Digital Currency」 Hastings Science & Technology Law Journal 4 (2011): 160-208ページ。http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857.

William J. Luther 「Cryptocurrencies, Network Effects, and Switching Costs」 Mercatus報告書、ジョージ・メイソン大学メルカトスセンター、バージニア州アーリントン、発行予定。https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134.

George Selgin「Synthetic Commodity Money」報告書、ジョージア大学経済学部、ジョージア州アテネ、2013年4月10日。http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.

Nikolei M. Kaplanov「Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation」 Loyola Consumer Law Review 25 (2012): 111-174ページ。http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203.

ヨーロッパ中央銀行「Virtual Currency Schemes」2012年10月。http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

著者略歴

ジェリー・ブリート（Jerry Brito）はジョージ・メイソン大学のメルカトスセンターにおける上級研究員であり、当センターの技術ポリシープログラムのディレクターです。彼はまた、ジョージ・メイソン大学にて、法律学の非常勤教授を務めています。彼の研究内容は技術とインターネットの政策、著作権、規制プロセスに焦点を当てています。彼の論説はウォール・ストリート・ジャーナル、ニューヨークタイムズ、その他に掲載されています。ブリートはスーザン・ダドリー（Susan Dudley）と共同でRegulation: A Primer, and the editor of Copyright Unbalanced: From Incentive to Excessを著しています。彼は技術、政策、経済の交差点に位置する、多岐にわたる著者、学者、起業家と密に議論を交わす30分のポッドキャスト、Surprisingly Freeを毎週配信しています。彼はまた、技術ー政策に関する有名なブログ、Technology Liberation Frontにも寄稿しています。彼は政府内の透明性と説明責任を推進するためにいくつかウェブサイトを立ち上げています。その中でもOpenRegs.comは連邦政府の規制記録資料編成システムを代替する手段を提供しています。ブリートは法務博士号をジョージ・メイソン大学の法学部にて取得し、学士号をフロリダ国際大学の政治科学部で取得しています。

アンドレア・カスティーヨ（Andrea Castillo）はジョージ・メイソン大学のメルカトスセンターにて、出費と予算戦略のプログラム助手を務めています。彼女はRandall G. Holcombeと共著で「Liberalism and Cronyism: Two Rival Political and Economic Systems」を執筆しています。Neighborhood Effectsでブログを執筆しており、The Ümlautのコラムニストでもあります。彼女はフロリダ州立大学の経済政治科学部で理学士号を取得しました。

メルカトスセンターについて

ジョージ・メイソン大学のメルカトスセンターは市場志向型の思想においては世界一流の大学です。アカデミックな発想と現実世界の問題の間に横たわる壁を乗り越えます。
大学に本拠地を置く研究センターとして、メルカトスは市場がどうやって人々の生活を向上させるかについての知識を広めます。大学院生をトレーニングし、調査を行い、社会の最も緊急な課題に経済学を適用して解決法を示唆します。
我々の使命は自由の発展に影響する組織についての知識と理解を広め、人々が自由に、豊かに、平和に暮らすための障壁を乗り越えるために継続して実行可能な解決法を探ることです。
1980年に設立されたメルカトスセンターは、ジョージ・メイソン大学のアーリントンキャンパス内に位置しています。
http://www.mercatus.org