

①標題	Bitcoin システムデータの基礎研究
②学部・学年	商学部・4 年
③学籍番号	1114204Y
④氏名	春田拓海
⑤連絡先	〒216-0035 神奈川県川崎市宮前区馬絹 3-6-18 080-5402-2338 takumi.haruta.919.dev@gmail.com

Bitcoin システムデータの基礎研究

1. はじめに

近年、暗号通貨を題材とする経済・ファイナンス分野からの研究は、増加傾向にあるが、暗号通貨特有のシステムデータを扱っているものはまだ少ない。システムデータは暗号通貨のパフォーマンスを測ることができる有用なデータであり、これらのデータを分析することによって、決済システムの効率性を解明し、改善・向上に繋がることが期待できる。本稿では、Bitcoin を題材として暗号通貨のシステムデータの時系列基礎分析を行う。

本稿の成果は2つある。1つ目は、暗号通貨システムの内部構成を「データ」という視点から把握できることである。本稿が、暗号通貨を対象とする他の経済学者の研究の下地となることが期待できる。2つ目は、暗号通貨のシステムデータが時系列的に応答し合い、データ自体に分析の価値があることを解明した点である。これは Chiu et al. (2018) 等で見られる「暗号通貨システムの最適デザイン研究」の有用性を補強する内容となっており、暗号通貨システム全体をモデリングが有効な手法であることの一つの根拠となる。

具体的な時系列分析の内容を最初に言及しておく。まず、Bitcoin のシステムデータを貨幣発行量が半減された日で3つに分割し、それぞれのデータ群に対してインパルス応答関数を用いて、変数のショックによる反応を調査する。変数間の関係性と、データの期間の違いという2つの視点からシステム構造を分析した。

構成は以下の通りである。2章で周辺分野の先行研究のサーベイを行い、3章で決済システムの面から従来の法定通貨と暗号通貨を比較検討した。4章では実際に、システムデータを扱って基礎分析と、変数間のショックによる反応を見るためにインパルス応答分析を行い、5章でまとめを行う。

2 既存研究

Bitcoin および Blockchain に関する既存研究は、初期は情報工学に関するものが多かったが、近年になり経済学・ファイナンスの視点からの研究も増えてきた。特に多く見られるテーマが、「Bitcoinの価格は何で決まるか」といった投資の観点からの研究である。しかし、貨幣論やネットワーク構造、トランザクションのボリュームに着目した研究も少なからず進められている。本章では、システム規模の指標となる「トランザクション」に着目し、既存研究を「交換媒体としての流通可能性」、「トランザクションのボリュームを扱った研究」の2つに分類して紹介する。次に4章での分析で参考にした、Ciaian et al. (2016) と Chiu et al. (2018) の研究を紹介する。

「交換媒体としての流通可能性」に関する既存研究では、Ammous (2018) や Baur et al. (2018) が挙げられる。Ammous (2018) では、5つの暗号通貨 (Bitcoin、Ethereum、Litecoin、Ripple、Steem) の貨幣的な特徴 (交換機能、価値尺度機能、価値貯蔵機能) をそれぞれの "Monetary policy" から分析し、マネーとしての機能を果たしているかどうかを評価している。暗号通貨の供給は融通が効かず、需要は激しく変動するため、どの通貨も購買力が不安定であり、価値貯蔵機能と価値尺度機能においても優位性がないため、マネーとして機能していないと主張した。しかし、5つの暗号通貨うち Bitcoin のみ、価値貯蔵として機能するポテンシャルがあると述べている。暗号通貨の価値は、プロトコルの仕様変更によって大きな影響を受けるが、Bitcoin では、マイニングに使用されたコンピュータリソースや電力といった経済的コストを考慮すると、プロトコル変更でコインを移動するリスクが高いため、長期的にも現在のブロックチェーンの仕様が維持されるいくことが予想できる。さらに、Bitcoin の貨幣成長率は今後も逡減して発行上限に収束してい

くため、インフレによって貨幣価値が下がらない。このため、Bitcoin は価値貯蔵手段として機能する可能性がある」と述べられている。一方、その他の暗号通貨は、デジタル貨幣の用途以外の目的で設計されていたり、通貨の価値がそのアプリケーションに人気度に依存していたり、第三者機関が介する完全ではない分散システムであったりという現状から、マネーとして機能する見込みはないとした。Baur et al. (2018) では、統計的なアプローチから、Bitcoin が交換機能、価値尺度機能、価値貯蔵機能として使用されているかどうかを分析している。結論から言うと、Bitcoin は貨幣の代替にも交換媒体にもなっておらず、特に交換機能と価値尺度機能の機能は保持していないとした。トランザクションやウォレットのデータ使用したユーザータイプの分析によると、Bitcoin のユーザーは投機目的で利用している人がほとんどであるが、一部のユーザーの間では交換媒体としても使用されているケースもあるということが判明した。

「トランザクション・ボリュームを扱った既存研究」は、Kondor et al. (2014) や Koutmos (2018)、Balcilar et al. (2017) が上げられる。Kondor et al. (2014) では、Bitcoin を題材としてトランザクション・ネットワークの構造やマネーの流れを分析している。実際のブロックチェーンからトランザクションデータを抽出・解析して、ネットワーク上のユーザー分布、相関関係やクラスターリングなど、経済物理学のアプローチから Bitcoin ネットワークの性質を紐解いている。Koutmos (2018) では、Bitcoin のリターンとトランザクション・アクティビティの連関を分析している。Bitcoin のネットワークに参加する個人が増えるほど、Bitcoin のエコシステム全体の価値が上がると予想し、トランザクション数とユニークアドレス数のそれぞれの変動ショックが Bitcoin の価格に大きな影響を与えていることを示した。Balcilar et al. (2017) は、トランザクション・ボリュームが Bitcoin のリターンやボラティリティに与える影響について分析している。実際のデータの非線形性や構造変化に対処するために、ノンパラメトリックな手法でグレンジャー因果性を調べ、取引活動が安定しているときに、ボリュームは説明力を持つと述べている。

次に、Ciaian et al. (2016) と Chiu et al. (2018) について紹介する。

Ciaian et al. (2016) では、Bitcoinの価格を左右するファクターを、Bitcoinの需要供給の価格原理、投資家にとってのBitcoinの魅力、グローバルなマクロファイナンスの状況の3つに分類し、VARモデルで短期的・長期的影響の分析を行った。うち1つ目と2つ目は、変動はあるもののBitcoinの価格に明白に影響を与えていたが、3つ目は長期的にみても価格との関係は見られなかった。本稿のモデルには Bitcoin のシステムデータが分析に使用されており、Bitcoinの経済の大きさを測るための「1日あたりのユニークトランザクション数」と「1日あたりのユニークアドレス数」、流通速度を測るための「Days Destroyed」といった変数をモデルに取り込んでいる。

Chiu et al. (2018) では、ブロックチェーンを基礎とする暗号通貨システムの最適デザインを研究することを目的とし、「暗号通貨システムの一般均衡マネタリーモデル」（以下、Chiu-Koeppelモデル）を定義している。Chiu-Koeppelモデルの特徴は、トレードやマイニング、暗号通貨そのものの価値をモデル内に内生化している点である。それにより、ブロックチェーンが保持しているシステムデータを用いて、暗号通貨のパフォーマンスを定量評価・比較でき、また、コンセンサス・プロトコルが異なる暗号通貨間での比較（例 Proof-of-WorkとProof-of-Stake）や、従来の現金システムとの比較（例 BitcoinとUSドル）も可能にしている。Bitcoin の暗号通貨システムに関わる様々なプレイヤーの動機をモデル化するために、Lagos and Wright (2005) のサーチ理論¹を応用してモデル化に取り組んでいる。Chiu et al. (2018) で挙げている暗号通貨システム問題点は、現在のブロックチェーン技術を基にした暗号通貨では即時決済・即時合意ができないため、マイナーによるトランザクションの承認を必要としている点であり、経済学的に見ると 1.4% の厚生損

¹ サーチ理論については、清水(2016) で包括的かつ丁寧に解説されており、合わせて参照されたい。

失に繋がっていると指摘している。それに対し、Chiu-Koepl モデルで検証した最適なコンセンサス・プロトコルに従えば、厚生損失が 0.08% 相当まで下がるとしている。具体的には、マイニング活動を減らすようなプロトコルに設計し、貨幣発行の上限を上げ、トランザクション手数料より貨幣発行によるマイニング報酬の割合を増やす、または Proof-of-Stake のような別のプロトコルを採用すれば、システムの効率性が改善されると主張している。

以上の先行研究と本稿が異なる点は、システムデータそのもので時系列分析を行ったという点である。シンプルな分析ではあるものの、データ自体に価値を見出させるような研究は過去に存在していない。

3. 法定通貨システムと暗号通貨システム

暗号通貨そのものの分析に入る前に、3章ではまず法定通貨と暗号通貨を比較検討していく。3.1 節では、貨幣を取り巻く「システム」という全体像から「法定通貨システム」と「暗号通貨システム」を比較・定義する。3.2 節では、「決済」の観点から両システムを比較し、暗号通貨システムの優位性を考察する。

3.1 システムの全体像の比較・定義

法定通貨システムは大きく分ければ、図3.1 のように「中央銀行」「民間金融機関」「家計・企業」「政府」の4つの主体で構成されており、それぞれが複雑に関与している。中心的存在である「中央銀行」は「発券銀行」「銀行の銀行」「政府の銀行」という3つの機能を持っている。中央銀行は「物価の安定²」を目標とし、一国経済の「おカネの蛇口」のような役割を担っている。時々の金融政策を通して、マネタリーベースを操作し、波及経路を通じて間接的に経済全体のマネーサプライを調節して、経済主体の安定した経済活動を支えている。その下で「民間金融機関」は、家計や企業に決済システムを提供し、円滑で効率的な経済活動を維持しているほか、信用創造によって、景気に左右される資金需要に応える役割を担っている。「家計・企業」は、一国の経済を動かす根源である。中央銀行は「政府」と独立³した関係でありながらも、整合性が取れるよう、互いに連携しながら経済・金融政策を進めている。

日本を例にして、さらに詳細に法定通貨システムを紐解いていくと、システムを支える機関・サービスが非常に多いことがわかる。物質的な面から見ると、まず法貨（現金）は、政府や日本銀行の政策のもと専門の機関で発行される必要があり、紙幣は国立印刷局で印刷され、硬貨は造幣局で铸造されている。こういった現金を安全に効率よく、正確に管理するためには、銀行業のATMや、小売業のキャッシュレジスター・自動釣銭機といった機械の開発も欠かせない。また、口座情報などを記録し、決済処理を行うためのITシステムも必要であり、日銀ネットや各民間金融機関システムでは、その運用・維持に膨大なコストがかかっている。さらに現代のグローバル経済において、法貨は一国内のみに留まらず、各国の外貨と取引が行われるため、その制度やルールを定め、外貨との決済システムを用意する必要がある。このように、法定通貨システムは現金とデジタル世界が混在し、その維持に多くの労力・コストがかけられている。

一方、Bitcoinをはじめとするブロックチェーン型の暗号通貨システムの構成は、法定通貨システムに比べればシンプルなものである。（図3.2）構成要素の分け方には様々な切り口があるが、大きく分けると、送金を行う「ユーザー（ウォレット）」と分散システム・ネットワークを支え

² 日本銀行法（平成九年法律第八十九号）第一章第二条より「日本銀行は、通貨及び金融の調節を行うに当たっては、物価の安定を図ることを通じて国民経済の健全な発展に資することをもって、その理念とする。」と記載がある。

³ 同法、第一章第三条・第五条より「日本銀行の通貨及び金融の調節における自主性は、尊重されなければならない。」「（中略）日本銀行の業務運営における自主性は、十分配慮されなければならない。」と記載がある。

る「マイナー（ブロックチェーン）」の2つである。「ユーザー」は送金金額と送金先のアドレス、マイナーに支払われる手数料を組み込んでトランザクションを発行する。「マイナー」は決められたコンセンサス・プロトコルの下で、ユーザーが発行したトランザクションの承認を行い、手数料とマイニング報酬をインセンティブとして得る。中央銀行のような中央集権機関は存在しないが、代わりにコンセンサス・プロトコルという「法」の下、各要素（ノード）は対等な立場でネットワークに参加している。法定通貨は銀行やクレジットカード会社といった第三者機関の仲介に依存しているため、その第三者機関のサービスが破綻すると経済に混乱をもたらすという、致命的なリスクがある。対して暗号通貨は、P2P技術を利用した分散型システムのため耐障害性に優れ、1つのノードがダウンしてもネットワーク全体が止まることはない。

暗号通貨に対して、アメリカ⁴、EU⁵、日本⁶の中央銀行は暗号通貨は通貨として普及しないという立場をとっており、中央銀行が独自の暗号通貨を発行する見通しはないと明言している。しかし、各国ともに暗号通貨の展望やその根本技術であるブロックチェーンの可能性については引き続き調査を進めていく方針を表明している。

3.2 決済システムからの比較

次に、両者を「決済手数料」と「決済処理」の2点から比較していく。法定通貨の決済システムとして、銀行・クレジット・デビット・電子マネーを取り上げ、暗号通貨の決済システムはBitcoinを取り上げて話を進める。

まず、「決済手数料」から比較する。日本の大手銀行の振込手数料は、送金金額や振込先によって金額は変わってくるが、総合すると一回に100円～900円ほどの手数料が発生する。また、カード決済や電子マネーは、売上に対して3%～10%の手数料が課されると言われている。手数料の負担について、口座振込は基本的に送金者が負担するが、カード決済や電子マネーは加盟店が負担している。

対して、Bitcoinの利用にかかる手数料は、送金者が支払うトランザクション手数料である。トランザクション手数料は送金金額ではなく、トランザクションのサイズである「バイト数」と、Bitcoinネットワークの市場原理に基づいて決定される。この市場原理というのは、コンピュータパワーやトランザクション全体の量、1ブロックに含めることができる容量が関係しており、ネットワーク上にトランザクションが溢れている場合、マイナーは手数料の高いトランザクションから承認し、ブロックに収める。手数料を0に設定することもできるが、手数料が極端に低いトランザクションは、承認が後回しになってしまうため推奨されていない。

表3.1は、Bitcoinのトランザクション手数料の年平均と年中央値を記した表である。トランザクション手数料は、BTC価格では全年で中央値・平均ともに0.001BTCを下回り、USDに換算すると、2017年終盤に爆発的に市場価格が上昇したピーク時以外は、10セント前後が相場となっている。Bitcoinの送金システムは、法定通貨と比べて手数料が安価であり、また送金金額に依存しないため、多額の送金を行う場合に魅力的な支払い手段である。しかし、手数料はトランザクションを発行する度に支払う必要があり、過度にトランザクションを発行すると、余計にコストがかかる仕組みになっている。このトランザクションの回数に比例する手数料の仕組みは、Bitcoin ネット

⁴ 2018年5月15日のDecoding Digital Currency Conferenceにて; <https://www.federalreserve.gov/newsevents/speech/files/brainard20180515a.pdf> (アクセス日: 2019年1月30日)

⁵ 2018年5月14日のThe 39th meeting of the Governor's Club Bodrumにて; <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html> (アクセス日: 2019年1月30日)

⁶ 2018年10月20日の日本金融学会 2018年度秋季大会における特別講演にて; http://www.boj.or.jp/announcements/press/koen_2018/ko181020a.htm/ (アクセス日: 2019年1月30日)

トワーク上に大量のトランザクションを発行して過度な負荷をかける攻撃者への対策になっているが、健全な利用者にとっては非効率な仕様である。この「手数料の設計」と「セキュリティ」はトレードオフの関係になっている。

表 3.1 トランザクション手数料の中央値と平均

	2012	2013	2014	2015	2016	2017	2018
中央値 (BTC)	0.00072	0.00079	0.00018	0.00017	0.00027	0.00079	0.00013
平均 (BTC)	0.00093	0.00079	0.00019	0.00018	0.00027	0.00095	0.00028
中央値 (USD)	0.00602	0.08278	0.09417	0.04444	0.16128	2.28266	0.82013
平均 (USD)	0.00757	0.10437	0.10057	0.04847	0.15748	4.81740	2.99569

次に、「決済処理」から比較する。法定通貨システムは現金や売上票といった現実世界のモノとの「接点」をまずは用意する必要があり、ここに多大な人的資本が割かれている。

ほとんど法定通貨の決済手段は、銀行口座間の送金を基盤としている。従来、口座振込は翌営業日に入金する仕組みであったが、2018年10月9日に全銀ネットが新しく稼働させたモアタイムシステムによって、このシステムに参加している金融機関の口座は、24時間365日即時振り込みが可能となり、早ければ即時、遅くても翌日に入金されるようになった。デビットカードとプリペイド式の電子マネーは、現金感覚で使用でき、即時に決済・入金が可能であるが、銀行口座間の送金機能の上に成り立っている。

クレジットカードの決済処理において、例えば Visa は、1秒間に 6万5千件のトランザクションデータを処理できるシステムを保持している⁷。しかし、購入から明細に反映されるまでの時間は、データ端末の種類や加盟店が売上票を送信するタイミングによって異なる。クレジットカード使用時は、カードの不正利用を防ぐためにカード発行会社へ取引に応じてよいか確認する「信用照会」のみだけ行われ、利用者の明細には反映されない。後日、加盟店が売上票をカード会社に郵送し売上データの確認が取れた後、利用明細に反映されるという仕組みになっている。そもそも加盟店にとって、決済処理を早く楽にすることがクレジット決済を導入する動機の一つにあたるはずだが、その仕組みからわかる通り、加盟店も決済システムを機能させる運用者となっている。銀行振込や電子マネーでは、第三者まで（送金者と受金者）が負担するコストは決済システムを利用する手数料のみであるが、クレジット決済では、手数料以外に売上票の管理や郵送といった決済システムの一部を担うコストも支払っているのである。このため、第三者までが負担するコストという観点では、クレジット決済は他の支払い手段と比べて非効率である。

対して暗号通貨は、そのネットワーク自体が決済システムであるため、法定通貨の決済システムに比べればシンプルである。決済処理はマイナーが担っており、決済速度は主にマイニング難易度によって調節されている。マイニング難易度は、トランザクションの承認時間やブロックの作成間隔を左右し、例えば Bitcoin は10分間隔、Ethereum は15秒間隔となるように難易度を調節している。難易度を低くすれば、ブロック生成間隔が短くなり、より高速に決済することができるが、ブロックチェーンの乱立（フォーク）が発生しやすくなり、不正やハッシュパワーの無駄遣いが起きやすくなる。この「決済速度」と「セキュリティ」のバランスは各暗号通貨で異なるが、人的リソースをほとんどかけることなく 24時間365日決済に対応している点は、暗号通貨一般で有位な特徴である。

⁷ <https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf> 参照。（アクセス日：2019年1月30日）

以上の議論を、表3.2 にまとめた。Bitcoin の決済システムのメリットは、手数料が低く送金金額に依存しない点や、24時間365日十分に早い承認速度で決済が可能である点が挙げられる。ただし、少額の送金でも必ず手数料が発生してしまうため、現物渡しで手数料のかからない現金決済と比べると見劣りする点もある。

表3.2 決済システムの比較

	暗号通貨 (Bitcoin)	口座振込	クレジットカード	デビットカード・電子マネー
構造	マイナーによる承認、コンセンサス・アルゴリズム	各銀行口座間で決済	信用照会、売上票の送信と確認	即時決済
手数料	平均・中央値 0.001BTC以下、ドル換算で10セント前後	100円～900円	3%～10%	3%～10%
負担者	送金者	送金者	加盟店	加盟店
何に対してかかるか	トランザクションのサイズ	送金額、振込先の口座の違い	加盟店の売上	加盟店の売上
決済速度	24時間365日決済、承認まで平均10分	24時間365日、早くて即時、遅くて翌日入金（モアタイムシステム）	データ端末や加盟店に依存、非即時、銀行口座に依存	即時決済・即時入金、銀行口座に依存

現在の電子決済で主流となっているカード決済は、利用者にとってはメリットが多いが、加盟店にかかる手間とコストは大きい。このクレジット決済の「手数料は加盟店負担」という特徴はかなり特異なものであり、購入者は暗号通貨決済よりクレジット決済を選択した方が、決済速度は遅いものの加盟店が手数料を負担している分、得をしているのである。このため、暗号通貨がクレジット決済に代替することはないと考えられ、暗号通貨経済を確立させるためには、商品・サービスの「売り手」が先行する必要があると考えられる。すなわち「売り手」が暗号通貨でしか決済できない商品・サービスを展開し、その供給が十分になったとき初めて、暗号通貨は「通貨」として購買力を持ち、決済手段としての需要が生まれると考えられる。そして、近年のeコマース市場の成長ぶりを考えると、インターネットネイティブの暗号通貨がその決済手段として選択されるていく可能性は大いにありうる。

4 Bitcoin システムデータの基礎分析

3章で「手数料の設計」と「セキュリティ」の関係や、「決済速度」と「セキュリティ」のバランスについて少し触れたが、どちらを取るか、何で代替するかという視点から、暗号通貨システムはさらに改善できる余地を持っている。まずは、4.1節で、Bitcoin のブロックチェーンを構成するデータ群の基礎分析を行い、これらのデータの可能性について追求する。4.2節で、インパルス応答関数を用いた時系列分析を行う。

データは、<https://www.quandl.com/data/BCHAIN-Blockchain> より取得する。Quandl.comでは経済・ファイナンスに関するデータを容易に取得できるサービスを提供しており、大元のデータは <https://www.blockchain.com/charts> からAPI経由で取得している。さらに、あらゆるBitcoin取引所で行われた1日当たりのすべての法定通貨との取引回数を、<http://>

api.bitcoincharts.com/v1/csv/ から取得したデータよりカウントし、市場取引の様子も調査した。システムデータの一覧は、表4.1 にまとめている。一番右の列「影響元」は、変数がどこから影響を受けているかを記した列であり、ユーザーの行動などの外生要因か、Bitcoinの Protokol仕様などの内生要因か、その両方かに分かれる。

4.1 システムデータの基礎分析

- **Bitcoins in Circulation**（発行されたBitcoinの総量）

Bitcoin の発行量は、マイニングによって生み出される各 Coinbase Transaction に記録されており、それを全て集計したものが "Bitcoins in Circulation"、法定通貨でいうマネーサプライである。図4.1 からは、貨幣発行量半減の日を境に Bitcoin発行量が半減し、総量が逡減していることが読み取れる。

- **Market Price**（Bitcoin市場のUSドル価格の主要取引所間の平均）と

Confirmed Transactions Per Day (No. Transactions)（1日のトランザクション数）

法定通貨の取引高（ボリューム）と異なり、Bitcoinのトランザクション数（ボリューム）は、金融取引だけでなく全ての送金データを記録している。図4.2 は USD/BTC 市場価格と "Confirmed Transactions Per Day" をプロットしたものであり、2012年月中旬からトランザクション数が増加し始め、市場価格の最高値に到達した日にかけて非線形に取引量が増加していることが読み取れる。USD/BTC 市場価格の極端な上昇はバブルとも捉えることができ、最高値 \$19,498.68/BTC からわずか1年で \$5,000/BTC を下回るまで価格が暴落した。市場価格の暴落に反比例してトランザクション数は再度増加している理由の一つに、Bitcoin が金融商品として見切りをつけられ、投げ売りされていることが予想される。データ上の特徴的な日を表4.1 にまとめた。

表4.1 Bitcoinマネーデータの重要な日

	日付	マネーサプライ	Bitcoin 資産総額	USD/BTC 価格
Bitcoin資産にドル価格がついた日	2010/8/17	3,744,250 BTC	\$287,933	\$0.0769/BTC
USD/BTCが初めて\$100を超えた日	2013/4/1	10,979,300 BTC	\$1,125,488,153	\$102.51/BTC
Bitcoin時価総額、USD/BTC価格の最高点	2017/12/17	16,746,025 BTC	\$326,525,438,567	\$19,498.68/BTC

- あらゆるBitcoin取引所で行われた1日当たりの総取引数⁸

図4.3 は、トランザクション数と Bitcoin 全取引市場の取引高を比較したものである。トランザクション数自体、図4.2 で見るように変動が激しいものであるが、全取引市場の取引高はそのさらに上を行っている。分析前の予想では、Bitcoinのトランザクション数から全取引市場の取引高を引けば、純粋な「交換媒体」として使われたトランザクションデータが得られると考えていた。しかし、グラフから察するに、取引所はある程度の期間を設けて、そこで起きた取引高を差し引きし、まとめて送金を送っているということが推測される。送金にはトランクション手数料がかかるため、取引所が余計な手数料を減らすために、まとまった送金が行われていると考えられる。

⁸ exchに関して、諸事情で 2017年12月31日までのデータしかカウントできなかった。

-
- **Estimated Transaction Volume**（お釣りを除いた1日のトランザクションのBitcoin量）と **Total Output Volume**（お釣りを含む1日のトランザクションのBitcoin量）

図4.4 において、"Estimated Transaction Volume" と "Total Output Volume" はどちらもトランザクションデータに含まれるBTC量の総量であるが、送金者に返されるお釣りを含むかどうかという点で異なる。そのため、少額の送金であっても、Inputに使われる金額が大きければ、その分お釣りが増え"Total Output Volume" は増加する。グラフでは参考程度に"Total Output Volume" も記したが、純粋な送金金額を見るには"Estimated Transaction Volume"の方が適切である。グラフからは、"Estimated Transaction Volume" は "Confirmed Transactions Per Day" の上昇具合と比べてトレンドが薄く、2011年ごろからすでに一定金額の取引が行われていたことがわかる

-
- **Number Of Unique Addresses Used**（総ユニークアドレス数）

図4.5 の "Number Of Unique Addresses Used" は、Bitcoinネットワークに参加しているアドレスの数を表し、ユーザー規模の参考になる。グラフからは、2013年頃から、USD/BTCの最高値の日に向けて右肩上がりに上昇していたが、直後の価格の暴落とともにユーザー数が激減し、2018年は400,000 ~ 500,000 アドレスの間で推移している。

-
- **Median Confirmation Time**（トランザクションの承認待ち時間）

図4.6 の "Median Confirmation Time" を見ると、ハッシュレートに対してトランザクション量が過度に多い2012年や2017年の承認待ち時間の中央値は10分を超えてしまっているものが多く、送金処理が遅延してしまう問題が発生している（スケーラビリティ問題）。このスケーラビリティ問題に対して、ブロックサイズの上限を上げること、ブロック生成間隔を短くすることといった「プロトコルの変更」による対策案を用いるか、「Segwit」や "Lightning Network" といった「技術的な手法」による対策案を用いるかという点で議論が展開されている。

-
- **Total Transaction Fees**（トランザクション手数料）

マイナーが受け取る収益は、新しく発行される Coinbase Transaction を基にしたマイニング報酬以外に、トランザクション手数料がある。図4.7 と図4.8 を見ると、トランザクション数が急増した2017年は、マイニング収益に対するトランザクション手数料の割合が増加したが、それ以外の期間においては、トランザクション手数料は微々たるものとなっている。マイニング報酬が1ブロックあたり 12.5BTC となった現在でも、マイナーにとってのインセンティブはマイニング報酬に依存しているということが読み取れる。

-
- **Hash Rate**（ハッシュレート）と **Difficulty**（マイニング難易度）

図4.9 と図4.10 は、マイナーのコンピュータパワー "Hash Rate" とマイニング難易度 "Difficulty" の関係を表したグラフである。"Difficulty" は "Hash Rate" が決定要因の一つとして作用しているため、ほぼ同じ推移の仕方をしていることがわかる。"Difficulty" が高くなると、個人のコンピュータでは組織的に運用している大規模なコンピュータ群に太刀打ちできなくなる。個々のコンピュータが協力して計算する「プール・マイニング」という手法で、個人のコンピュータでもマイニング報酬を得ることは可能であるが、「プール・マイニング」はコンピュータパワーがマイニング・プールに集中してしまい、分散システムの特徴を活かせないという問題を抱えている。

4.2 システムデータのインパルス応答分析

4.1節の変数が Bitcoin の決済システムとしてどう影響しあっているかを調査する。今回は、Chiu et al. (2018) の補強も兼ねて、Bitcoin の決済システムと関連しているシステムデータから、インパルス応答関数を用いて変数のショックに対するレスポンスを分析する。

分析では、4.1 節で紹介したデータより表3.7の変数をデータセットとし、モデルに組み込む。データの対象期間は貨幣発行量の変更日（2018年12月末時点で、2012年11月28日と2016年7月9日）に着目し、対象期間をPhase 1（2009年1月3日～2012年11月27日; 50 BTC / 10分）、Phase 2（2012年11月28日～2016年7月8日; 25 BTC / 10分）、Phase 3（2016年7月9日～2018年12月31日; 12.5 BTC / 10分）の3期間に分けた。貨幣発行量は、ブロック数の累計がある一定数に達すると半減するように設計されており、この設計によって Bitcoin のインフレが抑制されている。信用創造がある法定通貨と異なり、貨幣発行量のみがマネーサプライを決定しているため、Bitcoin の経済規模を説明するのに重要な指標である。

今回は、より直近の Bitcoin ネットワークの構造に着目するために Phase 2 と Phase 3 に絞り、変化率データのみに対してインパルス応答関数を用いた分析を行った。変数の接頭辞の "dl" は変化率データであることを示している。

表4.2 使用する変数一覧

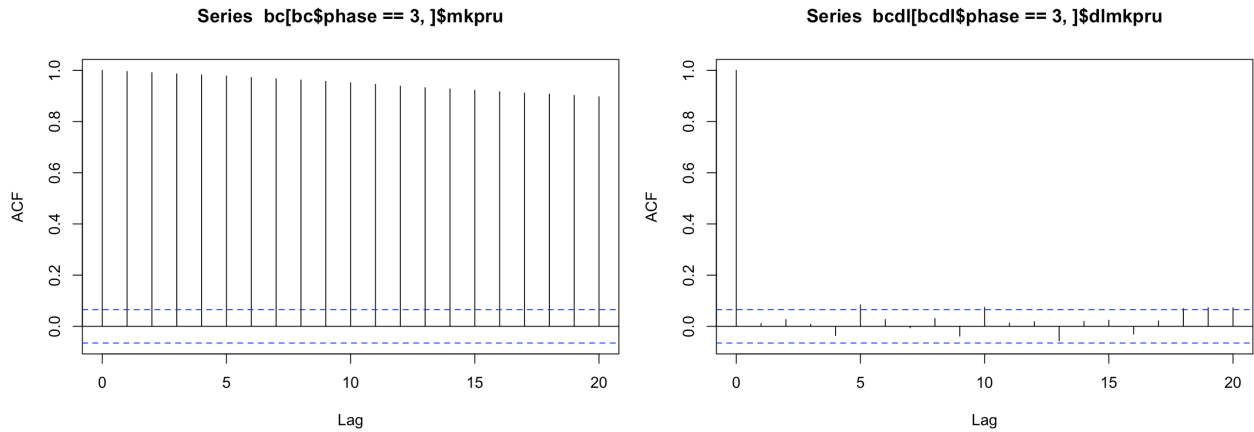
	変数名	表記名 / 変化率	単位	影響元
1	Market Price (USD)	mkpru / dlmkpru	USD	外生
2	Confirmed Transactions Per Day (No. Transactions)	ntran / dltran	個 (回)	外生
3	Number Of Unique Addresses Used	naddu / dlnaddu	アドレス	外生
4	Median Confirmation Time	atrct / dlatrct	分	両方
5	Total Transaction Fees	trfee / dltrfee	BTC	両方
6	Hash Rate	hrate / dlhrate	TH/秒	外生

まず、各変数の自己相関、単位根過程、共和分関係を調べる。沖本 (2010) に従い、自己相関の検定は Ljung and Box (1978) の統計量、単位根検定は ADF検定、共和分検定は Johansen 手法を採用する。

自己相関検定の結果では、Phase 2 はすべての変数で自己相関 = 0 の帰無仮説を95%点で棄却できない結果となった。しかしながら、Phase 3のデータにおいて、lmkpru のみ高い確率で帰無仮説を95%点で棄却できる結果となった。Phase 3 のUSD/BTC市場価格を、原系列と変化率のコレログラムと比較してみると、変化率で見るUSD/BTC市場価格は、ラグ1の時点で既に相関が弱くなっており、攪乱項の影響が強さが読み取れる。(図表 4.3)

図表4.3 変化率データ(Phase 3)の自己相関検定とコレログラム

	ラグ	1	2	3	4	5	6	7
dlmkpru	Q(m)	0.11	0.76	0.82	1.99	8.42	9.08	9.11
	P値	0.74	0.68	0.84	0.74	0.13	0.17	0.24



単位根検定はトレンド項あり、最大ラグ数を8に設定して行った。変化率に変換したことで、全ての帰無仮説が95%の棄却点で棄却できる結果となったため、全ての変数が定常性過程であると判断した。情報量基準にAICとBICを用いたが、情報量基準間で検定結果の差異は生じていない。

以後の分析では、よりラグ数の少ないBICに沿い、ラグを6に設定してVARモデルを組み、累積インパルス応答関数で、dlmkpru, dlnttranにおけるショックが、各変数に与える反応を調査していく。Phase 3のdlmkpruには自己相関が見られなかったが、定常性は満たしているためそのままVARモデルに組み込んだ。結果は図4.11～図4.14の通りである。

図4.11のdlmkpruのショックによる各変数の長期的な反応は、Phase 2では、dlnttran, dlnaddu, dltrfeeで0.01%～0.05%近くまで正の反応が見られるが、Phase 3になると有意ではない結果となった。図4.12のdlnttranのショックによる各変数の長期的な反応では、Phase 2・Phase 3ともに、dlnaddu, dlatrct, dltrfee, dlhrateで0.01%～0.06%近くまで正の反応が見られ、特にdlnadduとdltrfeeで顕著な反応をしている。Phase間で比較すると、Phase 3の方が、dltrfee以外の変数で反応が大きい。dlmkpruとdlnttran以外の変数のショックによる反応も、一部の変数間で存在した。まず、図4.13のdlnadduのショックに対するdltrfeeの反応について、Phase 2では0.005%程度の正の反応であったのが、Phase 3になると0.01%まで上昇した。また、図4.14のdlatrctのショックによって、dltrfeeに対して0.01%～0.02%の正の反応、dlhrateに対して-0.03%～-0.01%の負の反応が見られた。

算出された数値自体は、0.1%に満たないわずかな反応であったが、Phase 2からPhase 3にかけて構造が変化していることは読み取れる。また、Balcilar et al. (2017)では、ボリュームが価格に対して説明力を持っていると主張しているが、今回の分析ではdlnttranのショックによるdlmkpruに対する反応は見られなかった。

5. まとめ

4章の分析結果より、トランザクション数のショックに反応して、アドレス数と承認待ち時間、手数料、ハッシュパワーが上昇していることがわかった。トランザクション数はBitcoinでの経済活動を概観できる指標であり、これがBitcoinシステム内部にも負荷をかけているということが読み取れる。また、Phase 2からPhase 3に変わり、反応が大きくなっていることから、その負荷が上昇しているということがわかる。また、アドレス数のショックに対して、Phase 3で手数料が反応するようになったことから、ユーザー規模と手数料の関係が近づいたことが予想される。承認待ち時間のショックによって、手数料が増加しハッシュレートが減少する反応を示していることから、承認待ち時間の安定化もシステムの負荷を減らすために重要であると読み取れる。

以上、今回の分析からシステム全体を眺めると、Phase 3 以降手数料の重要度が増していると推測できる。手数料は、トランザクションサイズと市場原理によってその適正金額が定められているが、分析からトランザクション数やアドレス数、承認待ち時間のショックによって、手数料に反応が見られるように、より最適な市場原理のアルゴリズムを導入することで、少なからずシステム全体の効率化に良い影響が与えられるのではないかと考えられる。また、中でも承認待ち時間が作用している点から、マイニング全体の効率性も重要になってくる。結論として、Chiu et al. (2018) で見られる暗号通貨の最適デザイン研究は、暗号通貨システムの改善のために有用であると言える。

最後に、本稿の課題について言及する。まず、インパルス応答で得られた結果の値が非常に小さい点である。見方によっては誤差の範囲とされる可能性も高い。しかしながら、結果には「各変数と関連するシステムの機能」間の関係と整合性が取れていると考えられるため、今回は「反応があった」と解釈している。次に、対象データの期間の区切り方である。今回の分析では、マイニング報酬の半減日によって3つの Phase に区切ったが、この区切り方が経済構造の変化を捉えられているかは定かではない。最後に、今回の分析には VAR モデルを使用した。因果関係の分析までは着手できなかった点である。原系列データと論文では取り扱っていない対数値のデータは、単位根過程の変数を持ち、かつ共和分の関係にあったため、純粋に VAR モデルから因果性の分析をすることができなかった。そのため、今回は因果関係を調査せず、インパルス応答関数を用いて、ショックに対する反応のみを分析した。これらについては今後の課題としたい。

【参考文献】

- Daniel Kondor, Marton Posfai, Istvan Csabai, Gabor Vattay (2014), "Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network", PloS One 9, e86197
- Dimitrios Koutmos (2018), "Bitcoin returns and transaction activity", Economics Letters 167 (2018) 81–85
- Dirk G. Baur, KiHoon Hong, Adrian D. Lee (2018), "Bitcoin: Medium of exchange or speculative assets?", J. Int. Financ. Markets Inst. Money 54 (2018) 177–189
- Jonathan Chiu, Thorsten Koeppl, Bank of Canada, Queen's University, Victoria University of Wellington (2018), "The Economics of Cryptocurrencies – Bitcoin and Beyond", April, 2018
- Mehmet Balcilar, Elie Bouri, Rangan Gupta, David Roubaud (2017), "Can volume predict Bitcoin returns and volatility? A quantiles-based approach", Economic Modelling 64 (2017) 74–81
- Pavel Ciaian, Miroslava Rajcaniova, and d'Artis Kancs (2016), "The economics of BitCoin price formation", APPLIED ECONOMICS, 2016 VOL. 48, NO. 19, 1799–1815
- Saifedean Ammous (2018), "Can cryptocurrencies fulfil the functions of money?", The Quarterly Review of Economics and Finance 70 (2018) 38–5
- 石田良 (2018) 『仮想通貨に関する既存研究の整理』財務省 ファイナンス 2018 4月号 46-49
- 清水弘幸 (2016) 『分権的取引と貨幣の非中立性』
- Andreas M. Antonopoulos (2017) "Mastering Bitcoin: Programming the Open Blockchain 2nd Edition", O'Reilly Media
- 内田浩文 (2016) 『金融』有斐閣
- 沖本竜義 (2010) 『経済・ファイナンスデータの計量時系列分析』朝倉書店