Economic Bulletin of Senshu University
Vol. 52, No. 3, 167-182, 2018

《研究ノート》

サーベイ論文：非技術／情報系の経済系に仮想通貨・ビットコイン・ブロックチェーンをいかに教えるか*

小川　健**

＜要約＞

近年急速に注目される様になってきた仮想通貨とその暗号技術であるブロックチェーンは，経済系でも例えば金融方面を狙う場合には決して無視できない。また，その代表格の１つ，ビットコインはデジタルな金（きん）とも呼ばれ，その価格の乱高下・高騰以外にも中央銀行のないお金として経済学教育の教材にも充分なり得るだけでなく，教えないという選択は学生に「真実を伝えない」教育ともとれる。そして，こういう事柄を（10年前にはニュースに触れていなかった）学生が教員の手ほどき無しに勝手に学びだす際には，例えば10年ほど前に問題になった円天詐欺等のような項目に簡単に引っかかる危険性も高い。しかし技術系と異なり，経済系では例えば電子メール等での公開鍵暗号の仕組み等ですら教えられている訳ではなく，学生も多くは知らない。そこで，本報告では技術系ではない経済系では仮想通貨やビットコイン，そしてブロックチェーン等はどう教えたらよいか検討する。

JEL 区分：A22，E58，F31，F65，G12，G15
キーワード：仮想通貨，ビットコイン，ブロックチェーン，経済学教育，分散化

１．はじめに

公開暗号技術としてのブロックチェーンは仮想通貨のビットコインの登場と共にその仕組みとして技術／情報系には世に知られることとなり，10年近くが経つ。

経済系においてはキプロス危機等におけるビットコインの資本移動規制すり抜け手段としてその存在が知られるようになったと共に，金融論での説明に重要な役割を持つ，中央銀行のないお金（貨幣）として教育的な存在意義を持

＊本稿の作成に際し，橋本理博先生（帝塚山大学）及び高久賢也先生（広島市立大学）への討論者をお願いしています。この場を借りて御礼申し上げます。商標等侵害意図はありません。本稿にありうる誤りについては執筆者に帰します。（本稿は専修大学社会科学研究所　野口旭グループの支援を受けています。）

＊＊専修大学経済学部准教授

つ。経済系で就職の多い金融業界でもブロックチェーンは，手数料・費用引き下げ等の観点から国内外で注目されている。

一般でも2017年12月にはビットコインの（対US＄）年初比20倍とも言われる高騰や１日で（対US＄）約29%，５日で（対US＄）４割強の下落率が日本経済新聞（2017a，2017b）等の経済新聞等でも報じられ，三省堂（2017）での今年の新語2017にも第７位に仮想通貨が入る等，関心は高まっている。その反面，2014年の取引所・マウントゴックスの破綻が日本ではビットコインの仕組みを知られる前に起きてしまってビットコインという名前を初めて聞いた人も少なくなかったことから，ビットコインそのものに対する誤解した警戒感も日本では少なくない。

技術面以外でもビットコインや各種仮想通貨について扱う書籍は増えてきたが，国際金融を始めとする従来の科目への組み込みはまだ不十分である。しかし，2017年頃の価格高騰・乱高下等で一般にもその存在が知られ出し，シカゴ等で先物市場等が一部整備され，日本では木ノ内（2017）等で「仮想通貨法」とまで言われる改正資金決済法等が施行されたとともに，一般における手の出し易さもあるため，教育での扱い方も考察が必要になる。

ところで，ブロックチェーン技術に焦点を当てて説明できる技術／情報系と経済系では背景や教育目的が異なるため，取扱い方に関しても技術／情報系とは異なる方法が求められる。また，従来の講義に組み込む際にもどの科目にどう組み込むのが適切か等の検討も必要になる。そこで本講義では，国際経済・国際金融の学部２年次用初歩的な講義を中心に，関連講義も含めてどの項目をどう扱うべきか等の検討を行う。

第２節では項目内容の選別などを行うが，本稿は経済学教育のための内容選別を基にしているので，サーベイ論文としての位置づけを行う。旧聞に属する情報についてはあえて参考文献を挙げない場合もあるとともに，記載時の最新情報なども確認する必要があることから，ウェブログ程度の情報も敢えて扱う。最終節でまとめとする。

２．項目内容の選別とその理由

まず技術／情報系との背景の違いとしては，経済系ではプログラミングを仮定できない等，情報関係の知識が圧倒的に乏しい状態での講義が必要な側面がある。実際にプログラムを組んでブロックチェーン技術を体験する手段が取れない。

また，既存の仮想通貨を「買わせる」手段については，学生のお金を使わせることに対する警戒心等や（税法上の）雑所得扱いの問題もあり，シラバスでの成績評価方法に明記できない。従って，他の方法が求められる。更には，少し前の事象さえ知らない場合も多く，歴史的経緯や詐欺対策等も必要になる。

2.1　ビットコイン登場前の疑似通貨等との比較

まずは，ブロックチェーン技術が登場する前の疑似通貨，例えば仮想空間セカンドライフ（SL）[1]のリンデンドルや，日本では都市部を中心に馴染みの深いSuica（JR東日本）やEdy（楽天），nanaco（7&I HD），waon（イオン）等の電子マネー，詐欺に使われた疑似通貨の代表例である円天（L&G）等を取り上げながら，ビットコインを初めとする現代的な仮想通貨（暗号通貨）の持つ特徴やキャッシュレス社会との関連等を説明する必要がある。

2.1.1　課金・セカンドライフ（SL）のリンデンドル・分散型

旧聞のリンデンドル（SL）を紹介するのは，田下（2016）にもあるように一般のオンラインゲームの課金ではRMT（リアル・マネー・ト

1　セカンドライフ・ホームページ，https://secondlife.com/?lang=ja-JP（accessed 2017.12.28）

レード）や課金アイテム・ゲーム内通貨等の払い戻しが禁止・不能な例が多い。それに対し，リンデンドル（SL）では価値の変動を許せばUS＄や円等の主要通貨に払い戻せるからである。外部者にはこの違いの方が大きいが，セカンドライフが流行したのは2006–08年前後なので，歴史的事象と化している。そのため，課金は払い戻しが不可能で転売が禁止（違反者はアカウント凍結などの追放措置），というイメージが全てではないことを示すためにも，リンデンドル（SL）を紹介するのは意味がある。

梅津（2014）等でも指摘の様に，ビットコイン等現代的な仮想通貨（暗号通貨）との従来の仮想通貨・疑似通貨との大きな違いは管理機関が存在するか否かである。大河原（2014）等にもあるように管理機関がないため管理費は抑えられるが皆で監視できる分散型（P2P）のため堅牢になる等のブロックチェーンの特徴的性質の説明は重要となる。仮想通貨まとめ（2017）にもあるように，分散型の重要性はインターネットとの類推で説明できる。

2.1.2 なぜビットコインの安全性担保のPoWを講義で取り上げるべきではないか

経済学の講義で分散型に関して扱う先駆性・安全性についてはここまでに留めるとして，質疑応用対応や教員側の理解として，本来P2Pの技術はかつてファイル流出騒動を招いたWinny・Share等のファイル交換・共有ソフトでも使われていたものであり一部では逮捕者も出ているため，P2Pだから安全，ということは違和感を持つ外部者も多い可能性がある。

しかし，ACCS（2013）でも紹介されている様に，ファイル交換・共有ソフトはその多くがダウンロードしたものを自動アップロードする機能があり，本人が把握しきれていないまま著作権法違反に加担することが本質的な問題になったものである。これに対し暗号通貨におけるP2Pで記録されるものはビットコインを例にすれば，基本的にどのID・アカウントからどのID・アカウントへビットコインがどれだけ移動したか，の情報になるので，その情報が著作権法に触れるという訳ではない。なお，匿名性についてはCoinPost（2017a）等で紹介されているように，経路を伏せた上で「複数の鍵が無いと承認できない仕組み」（マルチシグ機能）を持つ匿名通貨のモネロ（XMR）や後述のZcash（ZEC）のように匿名性の高い匿名通貨も登場している。モネロなどは「裏切りや警察に押収された時など、特定の鍵を他の責任者が保有することで集めた資金を守」れることも知られている。そのため，匿名性についてはより高い匿名通貨が登場している，の段階に留めた方が（犯罪に繋がり易いため）よい。

その上で，安全性の「実質的」担保としてはビットコイン日本語情報サイト（2015）等でも紹介されているプルーフ・オブ・ワーク（PoW）の仕組みを紹介するのが望ましい。PoWはビットコインを始め（後述のリップル等を除く）多くの暗号通貨で取り入れられている手法で，「プルーフ・オブ・ワークとは、各取引を認証するために算出しなければならないデータまたはそのようなシステムのこと」と説明されている。ビットコイン等は取引履歴の集まりなので，取引の一部を改ざんしただけではすぐにおかしいと多くの人に分かってしまうため，履歴を遡って改ざんをしないと偽造ができない仕組みになっている。ゆえに，高橋（2017a）にもあるようにその後の取引まで全て改ざんが必要になるが，これには取引を証明とする採掘（マイニング）という作業での世界中の計算競争に打ち勝つ計算量を達成しないといけないことが知られていて，偽造が非常に難しいことが知られている。改良方法も各種提案されている。

PoWを経済学の講義で取り上げるべきではない理由として，「事実上」に依拠した不可能性がある。日本では経済学の学部生の多くは文系で入学してくる。そのため，技術／情報系より計算に対する経験・耐性が弱いことが多く，計算機の仕組みや限界なども通常は説明しない

ことから，機械に計算させるのに処理速度が有限ということを理解していない場合も珍しくない。そのため，計算量の関係で事実上不可能，という概念を理解し難い可能性が高い。従って，PoW の仕組みを説明したとしても，「絶対ではない」という部分に対する疑念が出てきたときに対処し難い。

更に言えば，現代国際金融史では1992年の UK に起きた「ポンド危機」という項目を教えることも関係する。国際金融の仕組みを世界で事実上初めて普及させた UK のイングランド銀行を敵に回して，民間の巨大資本（ヘッジファンド）が先導して空売り攻撃を仕掛けてイングランド銀行の当時の固定為替レート政策を放棄させた，という歴史的な事件である。この事件を教える中で，民間の巨大資本が本気を出して総力戦を仕掛ければ，読みを誤らない限り（政策を変える等の意味で）何でもできてしまう，という疑念を持たせる可能性が実はある。これを誤解すると，民間の巨大資本が総力戦を仕掛ければ，勝ててしまうのではないか，という発想を招いてしまう可能性がある。そのため，世界中で監視をするから，という程度に留めて，具体的な項目を講義で説明するのは控える必要がある。

2.1.3　仮想通貨の法律的な定義と暗号通貨

仮想通貨に関する日本での法律整備を分かり易く説明した金融庁（2017）によると，改正資金決済法（仮想通貨法）では，次の 3 つの条件を満たす「財産的価値」を仮想通貨と定義している。

1．不特定の者に対して，代金の支払い等に使用でき，かつ，法定通貨（日本円や米国ドル等）と相互に交換できる
2．電子的に記録され，移転できる
3．法定通貨又は法定通貨建ての資産（プリペイドカード等）ではない

この定義では先のリンデンドルに関しても，1. の捉え方次第（SL にアカウントを作ることで不特定の者が自由に参加できて，SL の中の様々なものの代金の支払いなどに使える）では仮想通貨となると考えられる（残りの条件は満たされている）。その一方で，電子マネーの多くは Edy（現・楽天）や Suica（JR 東日本），waon（イオン），nanaco（7&I HD）などのようにプリペイドカードに該当するので，仮想通貨には当たらない。ID（NTT DoCoMo）や QUICPay（JCB）など後払いを中心とした電子マネーについても，日本で電子マネーとされているものの殆どが法定通貨である日本円建てでの利用が中心のため，仮想通貨には当たらない。

もちろん，法律で仮想通貨をどう定義するかと，仮想通貨と一般に呼ばれているものには何があるか，の間には大きな違いがあり，その意味では仮想通貨をもう少し広く取る必要があると考えられる。

定義や源流という意味では，ビットコインとブロックチェーンが始まるきっかけとなった論文である Nakamoto（2009）の存在を忘れてはいけない。しかし，書籍上は取り上げる価値はあっても，経済学の講義で取り上げる意義は薄いと考えられる。それは，サトシ・ナカモト氏が誰であるかが未だに確定していないことが挙げられる。誰かに関する研究には，色々な答えがあったが，経済学の講義でこれを取り上げれば，確定していない以上誰なのか，という部分に興味が逸れてしまう部分があるからである。特にサトシ・ナカモト氏は日本人という設定があり，日本において文系の多い場所でこの設定を講義の中で話すと，こちらに神経が向いてしまい，その仕組みの理解に目が向かなくなる危険性が高い。

2.1.4　詐欺の可能性と管理団体の存在意義

分散型（P2P）という技術的な違いを除けば，ビットコイン等と電子マネーとの違いはレート変動だけに見え，管理団体があるものとして知

られているもの，例えば「カレンシー・ボート」型のテザーや片淵（2017）等で紹介されているMUFGコイン（三菱東京UFJ銀行系），仮想通貨ラボ（2017a）等で紹介されているJコイン（みずほ・ゆうちょ等），そしてペーター・ラン（2015）や真田（2017）等で紹介されているアトムコイン（ALI）[2]，等とは異なる。外部者には1Jコイン＝1円等に事実上固定のこれら企業・団体系の仮想通貨は，電子マネーとの違いは薄い。管理団体がおかしな事を行えば，使用分も戻るとされた円天（L&G）の様に詐欺に使われる[3]。なお，毎日新聞(2018)によると，1MUFGコイン＝1円のように全く動かない形で固定すると，電子マネーのように「銀行を介さずに100万円超の送金を禁じる資金決済法」に触れるため，MUFGコインではこの制限回避のためにMUFGコインの取引所を作る代わりにその参加者を利用者とMUFG（発行団体側）に留め，1MUFGコイン≒1円を実質的に担保する仕組みをとるため，類似のものに広がる可能性がある。事実上のレートの固定化は藤井（2014）等でいう「キャピタル・コントロール」に類似する仕組みで説明できる。

今では旧聞に属するL&Gの円天事件等を紹介するのは意義がある。仮想通貨には数多くの詐欺があるが，単に詐欺が多いとして説明しても説得力を持たない上に，詐欺の具体例をイメージできないと自分が騙される危険性があることを理解できない可能性が高い。本質的にはねずみ講の域を出ない筈の円天事件も，円天という疑似通貨をかませて説明することにより，多くの人が画期的なシステムとして騙された。1円を1円天に換えることで永遠に減らずに色々なものが買えるお金を手に入れた，として騙された例を話すことで，騙されないためにも本質的には典型的な詐欺の形態を理解しておく重要性を伝えることができる。また，1仮想通貨＝1円のような，固定での変換ができ戻せるような仮想通貨については，管理団体が存在しないとできないものであり，その管理団体の信頼性を注意深く見る必要がある，と言える。

関連して，ビットコインには個々の間柄同士でのやり取りが電子的に出来ることから，闇取引や資金洗浄に使われてきたとの指摘もある。しかし，法律が未整備な間は闇取引の格好の手段であった反面，（日本などで）法律整備がなされ，シカゴ等で先物市場が整備されるなど一般化されてきて，価格高騰や流行語化等で認知度が高まってきた中では，闇取引等に使えるメリットも少なくなりつつある。加えて，ビットコインは取引履歴が連なっている形になっているので，匿名性という観点ではやや劣る部分がある。闇取引や資金洗浄には匿名性は重要な観点であるが，CoinPost（2017a）等で紹介されているように[4]，現在は匿名性を強化した暗号通貨として，モネロや「ゼロ知識証明」と呼ばれる取引履歴などを外部公開せずにやり取りする方法を取り入れたZcashなどの匿名通貨が登場していて，闇取引や資金洗浄など犯罪色の強い取引は移っていくと考えられる。その意味では，闇取引や資金洗浄等に繋がるからビットコインは如何わしい，という指摘は既に過去のものとなりつつある。

2.1.5 リップル

GiantGox（2017）でも紹介されている，銀行間取引・送金仲介用の仮想通貨として注目のリップル（XRP）は，本来金融関係に進む場合にはビットコインより注意深く説明しておく必要がある可能性はある。しかし，リップルは管

2 ゲーム内の通貨を現金に換える，という発想から誕生したアトムコインについては一部で詐欺疑惑も立っているため，本稿ではアトムコインの正当性は保証しない。

3 L&Gによる円天事件の詳細については例えば国民生活センター（2017b）を参照。

4 より詳細には次のサイトが参考になる。https://bitcoin-yoro.com/altcoin/dashmonerozcash（accessed 2018.01.05）

理に金銭的な動機が弱いので踏み込まず，為替と付け替え，コルレス取引の意義を説明すれば，リップルについては（やや不正確だが）新技術を用いた送金仲介会社として理解させる方が経済学の学部生講義の中では良い。

その理由としては次のものが挙がる。リップルには利用者が管理を行う仕組みを用いているが，技術／情報系と経済系ではその捉え方に違いがあることが挙げられる。技術／情報系には元々 Unix や Linux をはじめとしたフリーソフト集合体の文化があり，利用者が無料利用する上で管理・改善提供をすることが当たり前という仕組みが一部にはあることを理解している。しかし，それは利用する側にも技術提供のスキルがあることが大前提であり，技術提供のスキルが無ければ単なるタダ乗りをするしかない。経済系の学生の多くはプログラミングの経験を経ていないので，技術提供の経験は無い人が圧倒的に多い。そのため，フリーソフトや無料のものはそれを利用するのみのタダ乗りか，警戒して使わない選択のどちらかが当たり前となっている。自発的提供を理解するには，協力ゲームや非協力ゲームを利用した NPO 等を理解させることが鍵となるが，ゲーム理論を応用した NPO の経済学的な理解の段階は学部上級～修士の段階と考えられ，経済学の学部用講義において感覚として理解することが困難となる。

踏み込むなら，正確ではなくても，次のように説明するのが適切と思われる[5]。なお，この段落の記載は注釈 5 で挙げた資料に対し筆者なりに解釈を加えた説明である。リップルには会社・ネットワーク・仮想通貨（XRP）の 3 つの意味があり，本来的には法定通貨にとって代わるためのものというよりは，銀行間送金等のためのものであり，個々人で一般商品を決済するためのものではない。そこでリップルという会社とその周辺団体が新技術を駆使して開発した新種の（銀行間送金などのための）金融ネットワークとして説明する。銀行間送金を行うときには同じ国の間なら中央銀行に相互の銀行が開いている口座同士で行い（内国為替の一種），国境を超えたり中央銀行が無い間柄だったりするならお互いの銀行に口座を持ちあってやり取りすること（コルレス取引）が知られている[6]。この内国為替やコルレス取引は経済学の用語として金融論の講義では説明の必要性はあるし，国際金融でも講義で取り上げる価値はある。国際送金等が，お互いに直接は口座保有の無い間柄なら，繋がる経路を探して幾つもの銀行を介する可能性があり，その分手数料も引きあがるし，日数もかかれば送金エラーが起きる可能性もある。そこで，リップルという会社とその周辺が全ての銀行を繋ぐような新種のネットワークを作り，そこに各銀行が口座を設けて電子的に付け替えを行うことで，数秒・瞬時に色々な銀行間で国際送金ができる。新技術を駆使した電子的な付け替えだけだから，本来的な手数料も従来の銀行間よりは少なくて済む筈である。そのリップル・ネットワークにアクセスするには手数料がかかるので，その手数料を多少なりとも下げたいなら，リップル（XRP）という仮想通貨を買って利用することになる。さらにそのリップル・ネットワークはクレジットカードやデビットカード，ビットコイン等他の仮想通貨の口座など，色々な金融にも広げる構想がある。手数料の安さや処理速度などで規格が広がって来れば，銀行等は関わらないという選択肢が取れなくなってくるので，金融業界に行く場合には知っておく必要があるし，このネットワークが必要不可欠になって来れば，自分たちが使うものの保全は自分たちで行うようになる。

5　正確な説明より分かり易さを重視した次のサイトを参考にしている。https : //okanefuyasuzo.muragon.com/entry/18.html（accessed 2018. 01. 05）

6　例えば https : //b.pasona.co.jp/boueki/teachme/928/を参照。（accessed 2018. 01. 05）

2.1.6　電子マネーとの比較と規格の分散

グループ毎の発行のものは，電子マネー規格が日本でも何種か分かれて使える場所が異なる様に，普及に課題が残る。Suica 等の交通系電子マネーが普及した 1 つには東京・大阪・名古屋・札幌・福岡で相互利用を可能としたからであり（これは DVD の事実上の規格統一と同様である），相互利用の範疇に含まれない後払いの機能を持つ関西の私鉄・地下鉄系の PiTaPa は（コンビニ等）交通系電子マネーの利用可能な場所でも使えない例もある。中には T カード（Tsutaya）・Ponta（リクルート）・R（楽天）・D カード（NTT DoCoMo）などといった日本の大手ポイントカードのように統一規格にまとまらないままそれぞれが多数派争いをすることもあるが，規格分散をしたままの場合はそれぞれに対応する必要が出て来るため，普及しない可能性の方が高い。

このため，MUFG コインや J コインなどについて，規格が分散している間はあまり普及しない可能性が高い。3 大メガバンクの 2 つがそれぞれ独自規格に拘っているうちは，また残りの三井住友銀行の動きなどが決まらないうちは，規格として残るものなどは分からない。従って，技術の進展可能性は述べても，デファクトスタンダードが決まるまで J コイン等の具体例の紹介は待つのも手である。

2.1.7　取引所と手数料，ICO，雑所得扱い

ビットコイン等の暗号通貨を手に入れるには取引所・販売所に口座を開設するなどして，暗号通貨を買うないし取引所などで交換により手に入れることから通常は始まる。取引所・販売所には色々なものがあるが[7]，例えば2017年末で日本最大手の bitFlyer や（他にはなかなかない匿名通貨 Zcash 等も含め）数多くの種類の仮想通貨を日本で扱える機会を設けてきた CoinCheck，日本における有名投資家が監修したことで知られる Zaif，世界最大級で日本にも進出してきた Binance 等が知られている。

取引所では売り手と買い手をマッチングさせる市場を提供するだけなので手数料は少ないが，販売所はその一方を販売所が手数料を入れて担うので，確実・即座に取引したいなら販売所であるが，割に合う取引は取引所でないと行えないことが知られている。場所ごとに扱う種類が異なり，手数料を考えた取引所・販売所選択が必要なことは FX 取引等と同様である。違いとしては，現在は FX 取引開始時の多くにマイナンバーを各地指定の方法での提出が必要なのに対し，仮想通貨の取引所・販売所に関してはマイナンバーが不要な所もまだある。ゼミナール等でゼミ生に体験させる際には，マイナンバーの提出の段階で学生各自のマイナンバーを取引所等に提出させる際に（どこにあるか学生が把握していない，下宿生が住民票の移転をできていなくて実家にある，保護者が確定申告などで本人の意識しない内に税理士などに預けてしまう等）困難を来たすことも多い。

また，ビットコイン等は取引所等に置いておく以外に，パスワード等を基に手元にアプリなどを入れて，ネットワークから切り離して管理をすることや紙での管理も可能である。取引所等に置いておく方法はパスワードを忘れても問い合わせられる反面，かつてのマウントゴックスのように取引所等のトラブルや，取引所等が攻撃に負けた場合には消失の可能性がある。手元で管理をする場合には後述するように，パスワードを忘れると暗証番号を忘れた金庫のように永遠に取り出せなくなるので，経済学の講義で実際の取引を紹介するときには，それぞれの管理方法で注意が必要になる上で管理方法の選択についても話をすることが望ましい。

小林（2017）によると，仮想通貨の取引は確定申告での雑所得扱いになることが知られている。確定申告は社会人になればその必要性は理解している場合が多いが，学生のうちは確定申

7　以下の記載は http : //investor-a.com/2527を一部参照している。（accessed 2018. 01. 06）

告が何かを知らない場合もあり，その一方で理解している場合には確定申告免除の範囲を超えている場合が多い。経済学の講義でこうした取引所・販売所等を紹介するときには，雑所得に対する確定申告が必要になる可能性を説明するのが大切になる。

仮想通貨の世界では他にも，クリプトコインポータル(2017)やブロックチェーンラボ(2018)に紹介されている様に，トークンと呼ばれる将来的に取引可能となる予定の記念品を発行して資金を集めるICOという資金集めの手段が知られている。トークンは将来的に上場するまで価値が高まれば取引可能になるが，詐欺も多く注意が必要となる。トークンは記念品のため，将来的に取引可能になるだけの人気になることもある反面，人気になるものは一握りにすぎず，目利きのような作業が必要になる。講義で扱う際には，あえて学生の大半には馴染みのない，一部の人にしか分からないマニア的な例えを次々出して，砂漠の砂の中から一握りの光る原石を探すような途方もない可能性を追い求めるような作業である，と説明することになる[8]。ICOを扱う際には，未公開株と同様の詐欺の可能性に加え，その手続きの手順等が法律で決まっていて，法律違反のICOに引っかかる可能性や，上場しない可能性もあることを指摘する必要がある。また，福島（2017）等でもあるように，中国大陸ではICOが禁止となり，仮想通貨による取引が地下経済化している。ルール整備の必要性は世界へと広がりつつある。

8　この例は時代にかなり左右されるので，例は逐一更新の必要がある。例えば数多ある高校・大学・社会人野球や独立リーグの中から将来メジャーリーグで活躍できる原石を探す，まだ奨励会にもいない数多ある将棋サロン等の中から将来の竜王・名人等を探す，数多くあるご当地アイドル・地下アイドル・ライブアイドルから将来のミリオンヒットやCM最多出場等を担える原石を探す等の例を，具体的な名前を挙げながらの説明となる。

2.1.8　2017年のビットコイン等の仮想通貨市場はバブルか，の論について

最後に，2017年のビットコイン等の仮想通貨市場はバブルか，という部分に対する補足を加える必要がある。年末には年初比20倍前後まで一時達したビットコイン市場については，宿輪（2017）や日本経済新聞（2017a）を引くまでもなく，バブルであるとの指摘は数多くの部分で出てきている。しかし，経済学の講義でバブルか否かを論じるのは2018年1月現在では少し待つことも手であると考えられる。まず，もしバブルである場合にも，バブルか否かは崩壊するまでは予測の域を出ない。そのため，確定的なことを言えないものに対し学部生用の講義で言及する場合には「バブルとの指摘も出ている」位しか述べられない。

しかし，次のことは知られているし講義でも言及に値する可能性はある。ビットコイン等主要暗号通貨の変動の分散は主要通貨に比べ大きかった以上，DIME（2018）の指摘のように，上がるだけの理由が説明できなければ下がる可能性はあることを認識する必要はある。また，分散が大きい場合にはリスク・プレミアムの割合も大きくなる。

そして，日本経済新聞（2017b）でも証拠金取引での強制売却に言及があるように，最大25倍の証拠金（レバレッジ）取引が可能な取引所もあるビットコインでは価格下落の際にいわゆる「損切り」に相当する強制売却に拍車がかかることが知られている。そのため，強制売却が僅かの変動でも起きるなら，下落が一時的に止まらなくなることは考えられる。25倍のレバレッジ取引については証拠金が無くなる4％の下落でも強制売却は知られているし，損切りは投資家自身で証拠金が無くなる水準よりもっと高めに設定することもあり得る。1日で約29%，5日で約4割の下落率を2017年12月等に記録している。

そもそも，一般論として損切りに対する強制売却は設定した水準で売却を自動的に判断する

ことはあっても，その設定金額で本当に売却できるかは分からない。１秒に満たない範囲での急落等の際には，強制売却の自動判断から売却成立までに価格が変わることもある。損切りによる強制売却は１つの手段として有効だとしても，損切りに言及するならその設定価格で本当に売却できるか分からないことを一般論として言及する必要がある。

2.2　ビットコインを取り上げる理由

2.2.1　デジタル・ゴールドとしてのビットコイン

仮想通貨の中で，講義内で紹介する種類は限る必要があるが，ブロックチェーンによる現代的仮想通貨の発祥や時価総額最大，オンラインに限らない一般店舗での利用可能性が最も大きい等の事由以外にもビットコインを中心に説明すべき理由がある。

１つはポッパー（2016）等でも指摘されている，ビットコインが「デジタル・ゴールド」と評される様に，金（Au）との類推が強い面がある。まず（宿輪（2017）のように一部には効いていないとの異説もあるが）発行総量に設定上の上限（約2100万 BTC）がある。近代国際金融史の項目として，金（Au）には国際金融の仕組みが整備された19世紀に国際金本位制を採用していた時代があり，金本位制では発行総量に上限があることが経済発展の阻害要因として知られていて，これを解決するにはゴールドラッシュのような金（Au）の総量を増やすしかない。ビットコインを世界的に法定通貨にすると同様の問題が起きる。

2.2.2　ビットコインの法定通貨化と資本移動規制

現状では主要通貨（US＄，€，日本円，UK£，中国人民元等）に対しビットコイン等の価値は変わり得る，「変動為替レート」の世界を考えることになる。

変動為替レートの世界では裁量的に貨幣発行量を増やす事こそ景気対策（短期的な国民所得の増加）には効果があり，公共事業などの政府支出には為替レートを変えても，景気対策効果は資本移動が不完全な部分の限定的な効果しかない事はマンデル＝フレミング・モデルとして藤井（2014）等の学部生の国際金融の教科書にも載る情報である。政策的に貨幣の量を変えられないが，2013年前後のキプロス危機等でもある様に，資本移動規制の抜け穴とされてきたビットコインを（強制通用力を持つ）国の法定通貨にすると景気対策が事実上打てなくなる事は小川（2016）により指摘されている。この部分は重要である。ビットコインについて中途半端に知ると，ビットコインを国の法定通貨にする方が望ましい，との誤解が出ることがある。このため，ビットコインを国の法定通貨にするのはそれだけのリスクを伴ってなお妥当と考える場合に限られることを伝えないといけない。暗号通貨を使えない人に対して「カレンシー・ボート」のようにビットコインを積んでおいてその分現金を発行する仕組みでも取る必要もある。現状のビットコインの浸透度合いを考えれば，US＄や€等を直接利用する形で為替レートを固定するよりそのリスクは大きい。

中央銀行のような管理団体がいないお金としてのビットコイン等には，政府や中央銀行等の判断で価値を勝手に減らされないように，という個々にとっての資産保全という側面もあった。実際に中央銀行のある法定通貨の場合は，中央銀行が（財政赤字補てんなどを理由に）政府の求めるままに貨幣を刷ってしまい急激なインフレを招いた例は第１次世界大戦後のドイツ等のような歴史的な項目に留まらず，近年のジンバブエ・ドル等でも起きている[9]。物価はあまり変わらなくても，為替レートに対する影響をもたらす政策は変動為替レートの世界では政府・中央銀行ともに取ることが出来ることがマンデ

9　例えば http : //www.huffingtonpost.jp/2015/06/12/zimbabwe-dollar_n_7574706.html にあるハフポストの2015年の記事を参照のこと。（accessed 2018. 01. 08）

ル＝フレミング・モデルでは知られている。為替レート上の通貨安が引き起こされ，外貨に対する購買力が落ちることもある。藤井（2014）等にも書かれているマーシャル＝ラーナー条件が成り立つ通常の範囲では，通貨安は輸出促進策としても知られているので，近隣窮乏化政策になってでも採用する可能性はある。実際に日本では2012年１月から2015年１月までの僅か３年間で名目実効為替レート（NEER）・実質実効為替レート（REER）ともに日本円が約32%の円安を記録している[10]。こうした政策による価値・購買力の低下から守るために中央銀行のいる法定通貨よりビットコイン等の暗号通貨を使う，という面も無視できない。

為替レートのあり方には変動為替レート，固定為替レート以外に，為替レートの安定と裁量的な金融政策を求める際に使うキャピタル・コントロールが知られていて，歴史的にはアジア通貨危機時のマレーシアや中国大陸で効果を発揮した等，危機対策に有名な手段である。しかし，個々の側からは自由に資本が持ち出せないのは（特に危機の際は）困る訳で，ビットコインは資本移動規制に対する抵抗・抜け穴として使われてきた。例えば，ビットコイン総合情報サイト（2017）等で指摘のキプロス危機，ビットコイン百科事典（2017）等で指摘のギリシャ危機，資本移動規制の強い中国大陸等で使われてきた背景があった。通信のみで銀行を介する必要も無いので国際送金に対する規制の回避策にも使われた。

10　BIS（Bank for International Settlement）の公表データによると，2010年＝100としてnarrowではNEERが2012年１月で112.77，2015年１月で76.63なので2012年１月＝100に直すと約67.95，narrowのREERが2012年１月で108.15，2015年１月で73.82のため2012年１月＝100に直すと約68.26となる。この値が小さい方が円安である表示法のため，名目・実質ともに約32%の円安となる。これはbroadでもほぼ同様である。データはBISのHP https : //www.bis.org/statistics/eer.htm?m=6%7C381%7C676を参照。（accessed 2018.01.08）

2.2.3　国際送金とビットコインと未確認取引

野口（2017a）にあるように，国際送金が安く済む点はビットコインの昔のメリットとして指摘されてきた。原理的にはビットコイン等の現代的な仮想通貨は取引履歴を以て現在の所在を示す仕組みなので，電子情報だけで銀行等を介す必要が無い分，本質的な送金費用は少ない。

しかし野口（2017b）で指摘されている様に，ビットコインの場合には第３者による取引の検証を以て取引成立となり，その検証費用もビットコインで支払われる。ビットコインの価格高騰に伴いその手数料も他通貨比では引き上がる上に，送金件数増加に伴う未確認取引の登場・増加や，検証に用いる消費電力増の課題（高橋（2017b）によるとVISAの約66倍の１回あたりの消費電力，Pinnington（2017）によるとデンマーク１国並みの総消費電力）も登場してその持続可能性まで疑われる一方，尾崎（2017）が指摘するように他の仮想通貨（アルトコイン）の登場・分裂・規格争いが始まる等，ビットコインの国際送金での手数料が安く済む利点は消えつつある。

2.2.4　マイニングとハードフォーク・分裂の説明方法

大石（2017）によると，ビットコイン等の取引検証に使われるマイニング（採掘）は本来的には暗号を解くようなコンピュータ処理が必要な作業である。そのための投資も各地で行われていて，J-cast（2018）によると計算量強化のためのクラウドの活用サービスなども登場しているが，中にはその計算量の確保を狙って見知らぬ他人のコンピュータを知らぬうちに利用するマルウェア（プログラム）を仕掛ける・インストールさせる問題も起きていて，問題となっている。経済学系には金（Au）の採掘の代わりに検証作業を第３者が行うことで検証手数料を貰っていて，それは監査の料金との類推で理

解できる点が重要となる。取引件数が増えてくれば，その検証も手数料を適切に払うものから行われ，取引件数等の増加に伴い，検証方法を巡っての意見の相違も出て来る。管理団体のあるものと異なり，分散型は意見の相違が貨幣の分裂を招く。

ハードフォークは分散型暗号通貨では基本的な用語なので高橋（2017c）等でも紹介されているが，従来との整合性を取らずルール変更をある段階から無理に行うハードフォークを説明するには，対義語であるソフトフォーク（履歴を遡ってルール改訂を適用する）などまで含めて説明をする必要がある。しかし，ハードフォークは分裂のときに主に行われることやソフトフォークは履歴や合意形成が困難であることから，ハードフォークの具体的な仕組みを伝えるより，日本円が（従来の日本円を引き継ぐ）東京円と（東京円とは以降別々にやっていく）大阪円に分かれる感覚と対比させる方が望ましい。

佐野（2017）でも紹介されている様に，ビットコイン（BTC）は2018年までに（かつて分裂して誕生した）ビットコインキャッシュ（BCH）をはじめ幾つものの分裂を繰り返している。このときに分裂して誕生した新しい仮想通貨に対して元々持っていた分量と同量を新規付与する習慣が出たことから，Business Infinity（2017）ではハードフォークによる分裂が「禁じ手」であったのに「打ち出の小槌」となっていることが指摘され，宿輪（2017）によるとビットコイン等の上限に実質的な意義が出ていないことが指摘されている。ここについては，上限が事実上突破されるには，それは同量の価値が誕生に際し生まれ，ある程度類似した役割を並立する場合が中心である。しかし，現在のハードフォークによる分裂の多くは，類似した役割が並立する状況とは言い難い。野口（2017b）によると，BCH とビットコインがマイナー（採掘者）に対する報酬の入り方や，受け入れ店舗数の圧倒的な差，つまりビットコインは送金等の受け入れ店舗がある程度は存在するのに対し（筆者注：決済可能な店舗数と理解すればよい）BCH には受け入れ店舗が2017年11月現在殆どない，「マイクロペイメント」つまり少額送金での利用可能性（高騰したビットコインは少額送金には向かない）等からビットコインと BCH の違い等を説明しているように，役割がかなり大きく異なるし，両者はマイナー（採掘者）の確保を巡っての競争が起きるとの指摘もされている。異なる役割を持つものが誕生していて，中には事実上価値を失っていくものもあり，上限がないというよりは「別のものが出てきている」を文字通り解釈する上で色々な事情で規格争いをする，とした方が適切である。規格争いの中でその歴史的役割が終えれば事実上参加者を失って無価値の履歴と化していく。規格争いについては，当初ビットコインより細かい部分を担えるようにとして存在していたライトコインが，BCH と争う形になったことが指摘されている[11]。規格争いについては結果がどうなるかは分からないため，具体的な争いの詳細言及は講義内では避けるべきと考えられる。

Pinnington（2017）にもあるように，金（Au）は本質的に価値を有するがビットコインは違う，との指摘が出る事がある。しかし，欲しがる人がいるかで価値を有するかは決まるため，（他の仮想通貨に置き換わる可能性はあるが）仮想通貨を否定する意味で本質的に違うとの指摘は当てはまらない面も指摘の必要がある（肯定的な意味での違いはある）。昔は金銀複本位制として，銀（Ag）にも通貨価値があったが暴落した事と対比すればよい。

ビットコインが（Putnam and Norland（2017）等のように一部疑問も出ているが，現在の乱高下を除けば）本来は金（Au）に近い価値貯蔵媒体を持つ側面は貨幣の特徴に近い。特に，取引所保管以外にも切り離してパスワードと共に管理可能であり，パスワード紛失に伴い使えな

11　例えば https://bitcoiner.link/6004.html を参照。（accessed 2018.01.06）

くなる面は，暗証番号の忘れた金庫が開かないのと同様であるが紹介の必要性は高い。

なお，ビットコイン等は数多くの分裂を行いつつあるが，（宿輪（2017）で指摘のように，日本の法律上は通貨とは異なるが）野口（2017a）でもその重要性が取り上げられているように，非オンライン店舗を含めた色々なお店で決済に使える可能性が増えている「キャッシュレス」の側面と対比させて考える上では，（一部減少の兆しもあるが）ビットコイン本体が材料としては望ましい。

ビットコインを初めとする暗号通貨等の仮想通貨はクレジットカードやデビットカード，そして日本では電子マネーと共にキャッシュレス社会の構築上重要になる。

2.2.5　先渡・先物市場確立

CoinPost（2017b）にもあるように，ビットコインにも先渡・先物等のデリバティブ取引が始まった。日本経済新聞（2017a）でも指摘のあるように，近年の金融危機でも見られない1日で28.7%の下げ幅等も記録したビットコインでは，先渡・先物市場が登場することで価値の変動リスクを個々で管理可能になった。

2.2.6　仮想通貨の発展可能性

福島（2017）やSedgwick（2017）にもあるように，中国大陸での仮想通貨による資金発行調達（ICO）の禁止通達を初めとして，ボリビア等や一部イスラム圏を初め，公式にはビットコインが禁止の国も出てきて地下経済化の指摘もある。中にはエクアドル等のように，仮想通貨は自国管理下に置くため，という国も出てきている。天野（2017）で指摘のある様に，エストコイン等国家が発行する仮想通貨構想もあるが，国家発行のものは技術の進展として経済学上は法定通貨等と大きな違いはない。

他の仮想通貨としては取引量と特徴からイーサリアムが望ましい。BITPoint（2016）にもあるように独自のプラットフォームを作れてスマートコントラクト可能な面が特徴だが，経済学の講義ではスマートコントラクトの詳しい仕組み自体よりは，Suica等の交通系電子マネーで自販機の飲み物を買う例で類推可能になることを説明した方がよい。つまり強制的に決済が成立し，記録が電子的に残る。また，ブロックチェーンの利用可能性を広げるサイドチェーン（側鎖）の可能性を部分的に示した面は改良型暗号通貨の登場等その後の発展にも繋がる。

ブロックチェーンには暗号通貨以外にも様々な可能性があり，その経済的な潜在価値は高い予測が数多くでなされている。しかし，その可能性についてはまだ具体像が確定していないだけでなく，様々な予測の抜け落ち等も考えれば，広がってきた段階で改めて取り上げることになる。しかし，フィンテックの範囲を超えてブロックチェーンが使われ出したとき，その用途は経済学で取り上げる範疇を越える可能性が高い。

3．おわりに

現代的な仮想通貨としての暗号通貨に留まらず，その技術としてのブロックチェーンは，今後もますます多くの進展を見ること自体は疑う余地もない。しかも，それが技術／情報系だけでなく経済系でも知っておくべき案件になってきた。そこでは，何を学び，何を委託するのか，もっと言えば技術／情報系と十分に情報交換が出来，最低限でも業務委託などが出来る程度には理解すると共に，経済ならではの特徴を押さえて技術／情報系へ適切な依頼ができる様にすることこそが，経済系の人間がこの大きな変化を学ぶ理由となる。最早「今の動きが収まるまでは取り上げるべきではない」と言っていられる状況ではない。しかし，暗号通貨関連の重要性説明は既存の経済学とは切り離した説明も多く，既存の経済学教育への組み込みこそが課題となる。

本稿では国際金融／国際経済の学部2年次の初歩的な講義などを通して，これらをどのよう

に扱うかについての考察を加えた。時代の進展によって陳腐な情報となるかもしれないが，本稿が既存の学問体系・講義体系との整合性を取るための一里塚としての整理になればと考えている。

参考文献

日本経済新聞：“仮想通貨バブルに転機　ビットコイン，１日で29%急落”，日経電子版2017年12月24日（2017a），https：//www.nikkei.com/article/DGXMZO25012120T21C17A2EA5000/（accessed 2017.12.29）

日本経済新聞：“ビットコイン下げ加速　５日で４割超”，日経電子版2017年12月22日（2017b），https：//www.nikkei.com/article/DGXMZO24975170S7A221C1EA2000/（accessed 2018.01.05）

三省堂：“三省堂　辞書を編む人が選ぶ「今年の新語2017」「今年の新語2017」の選考結果”，三省堂（2017），http：//dictionary.sanseido-publ.co.jp/topic/shingo2017/2017/best10.html（accessed 2018.01.05）

木ノ内敏久：“仮想通貨とブロックチェーン”，日経文庫（2017）

金融庁：“平成29年４月から「仮想通貨」に関する新しい制度が開始されます。改正資金決済法等の施行”，金融庁（2017），http：//www.fsa.go.jp/common/about/20170403.pdf（accessed 2018.01.05）

国民生活センター：“国民生活”2017年６月号，国民生活センター（2017a），pp. 11−13　http：//www.kokusen.go.jp/pdf_dl/wko/wko-201706.pdf（accessed 2018.01.05）

Nakamoto Satoshi：“Bitcoin：A Peer-to-Peer Electronic Cash System”，（2009），https：//bitcoin.org/bitcoin.pdf（accessed 2018.01.05）

小林義崇：“‘‘利益の半分は税金”ビットコインの注意点”，President Online 2017.11.24（2017），http：//president.jp/articles/-/23637（accessed 2018.01.05）

田下広夢：“メルカリ問題―RMTがゲーム業界にとって困る理由”，AllAbout趣味（2016），https：//allabout.co.jp/gm/gc/466683/（accessed 2017.12.28）

梅津信幸：“ビットコインは「セカンドライフ」の仮想通貨と何が違うのか？”，SBクリエイティブOnline（2014），http：//online.sbcr.jp/2014/03/003712.html（accessed 2017.12.28）

大河原克行：“Bitcoinにみる，分散型仮想通貨の仕組みと課題”，Internet Watch（2014），https：//internet.watch.impress.co.jp/docs/news/649202.html（accessed 2017.12.28）

仮想通貨まとめ：“仮想通貨はインターネットの発祥理由と似ている”，（2017），http：//virtualmoney.jp/I0001233（accessed 2018.01.02）

ACCS：“WinnyやShareを使わないで！”，コンピュータソフトウェア著作権協会（ACCS）（2013），https：//www2.accsjp.or.jp/books/pdf/file_sharing.pdf（accessed 2018.01.05）

ビットコイン日本語情報サイト：“プルーフ・オブ・ワーク”，（2015），https：//jpbitcoin.com/about/term/proof_of_work（accessed 2018.01.05）

高橋諒哲：“プルーフ・オブ・ワーク（PoW）を少し詳しく！”，とってもやさしいビットコイン（2017a），http：//www.tottemoyasashiibitcoin.net/entry/2017/01/09/163336（accessed 2018.01.05）

片渕陽平：“三菱UFJ，仮想通貨「MUFGコイン」初公開　スマホアプリで送金”，ITmedia（2017），http：//www.itmedia.co.jp/news/articles/1710/02/news105.html（accessed 2017.12.28）

仮想通貨ラボ：“Jコインとは？～みずほ・ゆうちょ・地銀連合の仮想通貨”，仮想通貨ラボ（2017a），http://crypto-currency.site/?p=1802（accessed 2017.12.28）

ペーター・ラン：“仮想通貨アトムコインの秘密　賢い人からはじめてる，仮想通貨投資術”，LUFTメディアコミュニケーション（2017）

真田孔明：“Mastercardでの決済が可能となる仮想通貨アトムコイン”，生涯収入５億円倶楽部（2017）https：//5oku.com/level/level010/vc-basic/atomcoin/（accessed 2017.12.28）

国民生活センター：“L&Gによるマルチ商法的な巨額詐欺事件における上位会員の不法行為責任”，国民生活センター（2017b），http：//www.kokusen.go.jp/hanrei/data/201704_1.html（accessed 2017.12.28）

毎日新聞：“独自仮想通貨　三菱UFJが取引所開設へ　価格安定図る”，毎日新聞電子版　2018年１月14日付（2018），https：//mainichi.jp/articles/20180114/k00/00m/020/098000c（accessed 2018.01.14.）

CoinPost：“仮想通貨の法律整備から匿名通貨が窮地に立たされている理由を考える”，仮想通貨ニュースサイト―CoinPost（2017a），http：//coinpost.jp/?p=9157（accessed 2018.01.05）

GiantGox：“ビットコインとリップル（XRP）のたったひとつの大きな違いとは”，Ripple総合まとめ（2017），http：//gtgox.com/cryptopayments_info/the-difference-between-bitcoin-and-ripple-xrp/（accessed 2018.01.02）

仮想通貨ラボ：“J コインとは？～みずほ・ゆうちょ・地銀連合の仮想通貨”，仮想通貨ラボ（2017），http : //crypto-currency.site/?p=1802（accessed 2017. 12. 28）
クリプトコインポータル：“ICO（Initial Coin Offering）とは？ICO スケジュール，ICO の参加注意点，仮想通貨取引まで”，（2017），http : //cryptocoinportal.jp/ico/（accessed 2018. 01. 06）
ブロックチェーンラボ：“トークンとは何なのか？暗号通貨とトークンの関係”，（2017）https : //www.blockchain-labo.jp/cryptocurrency/token（accessed 2018. 01. 06）
DIME：“ビットコインがなぜ，値上がりするのか説明できる？”，小学館（2018），https : //dime.jp/genre/495352/（accessed 2018. 01. 07）
ナサニエル・ポッパー：“デジタル・ゴールド―ビットコイン，その知られざる物語”，日本経済新聞出版社（2016）
宿輪純一：“ビットコインの「バブル体質」はどうやったって解消できない”，現代ビジネスメディア，（2017）http : //gendai.ismedia.jp/articles/-/53927（accessed 2017. 12. 28）
藤井英次：“コアテキスト　国際金融論　第 2 版”，新世社（2014）
小川健：“学部生の国際金融の教科書にも書ける，ビットコインを法定通貨にすべきでない理由”，専修大学・社会科学研究所・月報，第633号，pp. 37–46（2016）
ビットコイン総合情報サイト：“キプロス危機とビットコイン”，ビットコイン総合情報サイト（2017），https : //bitcoin-joho.com/knowledge/871.html（accessed 2017. 12. 28）
ビットコイン百科事典：“自国の金融危機から【ビットコイン】で資産を守った人たち”，ビットコイン百科事典（2017），http : //xn--eck3a9bu7cul.pw/articles/wf8KV（accessed 2017. 12. 28）
野口悠紀雄：“銀行の海外送金システムがもはや「時代遅れ」の理由”，Diamond ONLINE（2017a），http://diamond.jp/articles/-/128457（accessed 2017. 12. 28）
野口悠紀雄：“ビットコイン消滅も，送金コスト高騰問題の行方”，Diamond ONLINE（2017b），http : //diamond.jp/articles/-/150612（accessed 2017. 12. 28）
高橋諒哲：“マイニングの消費電力はどのくらいか　ビットコイン普及の課題”，とってもやさしいビットコイン（2017b），http : //www.tottemoyasashiibitcoin.net/entry/2017/12/22/145159（accessed 2017. 12. 28）
Pinnington Rebecca : “SHOCK CLAIM : Bitcoin is DESTROYING the planet and uses as much energy as DENMARK”, Express（2017），https : //www.express.co.uk/news/science/888535/bitcoin-environment-destroying-planet-fossil-fuels-energy-electricity-Denmark-US-2020（accessed 2017. 12. 28）
尾崎也弥：“「ビットコイン，永遠でない」“省電力”通貨登場も”，Nikkei Style（2017），https : //style.nikkei.com/article/DGXLASFL14HD2_V10C17A9000000?channel=DF150620172611（accessed 2017. 12. 28）
大石哲之：“大石哲之のビットコインの仕組み入門（1）ビットコインの発掘とは実際には何をしているのか？”，日本デジタルマネー協会（2017），http : //www.digitalmoney.or.jp/2013/12/bitcoin-sikumi1/（accessed 2017. 12. 28）
J-cast：“仮想通貨の採掘に他人の PC を無断利用　気づかぬうちに不正ソフト侵入，対策は...”，J-cast News 2018年 1 月 2 日版（2018），https://www.j-cast.com/2018/01/02317527.html?p=all（accessed 2018. 01. 06）
高橋諒哲：“ハードフォークとは”，とってもやさしいビットコイン（2017c），http : //www.tottemoyasashi-ibitcoin.net/entry/2016/10/14/113708（accessed 2017. 12. 28）
Business Infinity：“ビットコイン（BTC）分裂でもらえる仮想通貨【2017年12月～2018年 1 月】ハードフォークの最新予定時期をチェック！”，（2017），https : //business-infinity.jp/bitcoin-hardfork/（accessed 2018. 01. 06）
佐野祥貴：“仮想通貨取引所のビットコインのハードフォーク対応まとめ”，finte（2017），https : //www.enigma.co.jp/media/page-16934/（accessed 2018. 01. 06）
Putnam Bluford and Erik Norland：“ビットコイン，金と不換通貨の進化する経済”，CME グループ（2017），http : //www.cmegroup.com/ja/education/featured-reports/evolving-economics-of-bitcoin-gold-currencies.html（accessed 2017. 12. 28）
CoinPost：“ビットコイン先物について知っておくこと”，CoinPost（2017b），http : //coinpost.jp/?p=9755（accessed 2017. 12. 28）
福島香織：“中国「仮想通貨資金調達禁止」のインパクト”，日経ビジネス Online（2017），http : //business.nikkeibp.co.jp/atcl/opinion/15/218009/091100117/（accessed 2017. 12. 28）

Sedgwick Kai：“Five Countries Where Bitcoin is Illegal”, Saint Bitts LLC.（2017），https : //news.bitcoin.com/police-bust-turkish-gang-kidnapped-wealthy-bitcoin-holders/（accessed 2017. 12. 28）
天野透：“エストニアの電子通貨「エストコイン」構想を担当大臣が明かす”，ASCII（2017），http : //ascii.jp/elem/000/001/609/1609913/（accessed 2017. 12. 28）
BITPoint : “イーサリアムの特徴とは？ビットコインにはない優れた機能”, BITPoint（2016），https : //www.bitpoint.co.jp/column/tips05/（accessed 2017. 12. 28）

追記

（本追記は参考文献表記を一部除き省略する）：

本原稿提出後，匿名通貨を含む数多くの種類の仮想通貨の扱いが金融庁で審査中だったみなし仮想通貨交換業者 CoinCheck から仮想通貨 NEM（XEM）の大規模盗難事件が起き[1]，日本円での補てんが発表された[2]。オンライン（ホットウォレット）での一括管理や，NEM 財団から提示のあった複数鍵への対応が遅れたなど販売所側のセキュリティの甘さが指摘されている反面，匿名通貨 Dash への資金洗浄等も一部では指摘がある[3]。現物返却されない点やその評価額（Zaif の情報を基に加重平均で算出）への不満，強制売却扱いによる課税の問題など数多く指摘がある。その反面，過去の別の取引所等の流出していた全ての人の保管分で損害を均等割りして補てんした等[4]，対処策もバラバラである。金融庁の監督体制も強化が予想される。

かつてはイーサリアムの盗難（DAO 事件）に対するハードフォークのように「盗難を無かったことにする」ルール変更もあるが[5]，ルール変更による対処に反対する側による分裂でイーサリアム・クラシック（ETC）が誕生する等，ルール変更が最善で合意の取れる解決策でもない。

取引所・販売所など交換業者への攻撃・流出事件は世界中で起きていることから[6]，ネットから切り離した持ち運び可能な機材を利用したハードウォレット，紙に QR コードを印刷するペーパーウォレット等のコールドウォレットによる個人管理の重要性が指摘されている。これは自分の仮想通貨を自分で使う権利との兼ね合いで議論されることがあるが，紙はその紙の紛失に注意する必要があり，ハードウォレットはパスワードを忘れれば暗証番号を忘れた金庫の如く使えなくなる危険性も忘れてはいけないことは本文でも指摘した点である。

それ以上に，１つの取引所等に保管を集めない，分散の重要性をここでは指摘する必要がある。１つの籠に全ての卵を入れない等は金融工学の初歩，分散投資・分散管理の重要性であるが，銀行と異なりペイオフ制度がない以上，扱う取引所等を分ける必要がある。１つが攻撃で流出騒動を起こすと戻ってこない場合以外にも今回の CoinCheck のように他も出金停止等になりうることを考えると，分散は重要である。

今回の流出事件では流出した NEM の追跡を ID 単位で行うことが出来ていることに大きな特徴がある[7]。外部から取引履歴を丹念に追え

1　詳しくは http : //ur0.work/IrKQ 参照。（accessed on 2018. 02. 08）
2　http : //ur0.work/IrKh 参照。（accessed on 2018. 02. 08）
3　http : //ur0.work/IrK8参照。（accessed on 2018. 02. 08）
4　http : //ur0.work/IrL4参照。（accessed on 2018. 02. 08）
5　https : //moblock.jp/articles/17289参照。（accessed on 2018. 02. 08）
6　http : //ur0.work/IrLZ 参照。（accessed on 2018. 02. 08）
7　http : //ur0.work/IrNx 参照。（accessed on 2018. 02. 08）

ることに匿名通貨が登場してきた背景があることは本文で述べたが，今回は一部ホワイトハッカーによるマーキングが出来ていることから，IDと本人とのリンクが換金等で出来てしまうと足がつく危険性が高い。これはNEMが（匿名通貨ではないので）IDによる履歴公開がなされていること，IDと本人（犯人）の関連付けは（取引所等の口座でもない限り）換金まで難しいことを意味していて，有名ではない種類の仮想通貨の多くで当てはまる所と考えられる。

CoinCheck流出騒動以外にも多くの動きを指摘する必要がある。まず，クレジットカードによる仮想通貨の購入に対し制限・禁止の動きが強まっている。仮想通貨を1商品ではなく換金性の高いものや変動リスクの高いものとしてみている様子が見て取れる[8]。クレジットカードのキャッシング枠の現金化の問題や，手数料の高さ等の一般的な問題点を指摘する必要がある。

次に，改良型仮想通貨が数多く登場している面を指摘する必要がある。例えば，bitFlyerに今度登場したLISK（LSK）はCoinCheckで取り扱いがあったものだが，イーサリアム同様にスマートコントラクトを備えている反面，その設定をするプログラミング言語にJavascriptという有名なものが扱われていること，サイドチェーンの活用においてイーサリアムより優れていること等が指摘されている[9]。先のNEMにしても[10]，改良版ではC++という有名なプログラミング言語で扱えること，PoWより消費電力を抑えた取引の決定方法を利用できていること，そして「投げ銭[11]」やWeChatという中国大陸で有名なアプリでの送金が可能なことなど，ビットコインやイーサリアム等での問題点を改良した仮想通貨が数多く登場していることは注目に値する。その意味では，将来もビットコインが最も重要な仮想通貨であるとは言い切れない。

一方，仮想通貨での取引は世界的には規制の方向に向かいつつあることも指摘の必要がある。一時は200万円を超えていたビットコインの価格が100万円を再度割り込むなど，バブル崩壊の指摘も出ている。数学者の中ではビットコインの価値を「伝統的な方法で特定できる価値のない資産」と指摘する動きも現れ[12]，ビットコイン等の値動きの激しさはイスラム教では禁止の射幸性ある賭博に扱われる指摘が出始めた[13]。インド財務省ではビットコイン等の暗号通貨をポンジ・スキーム（ねずみ講）と指摘し[14]，韓国では韓国内全ての仮想通貨取引所の閉鎖を検討している旨法相発言があり[15]，BIS（国際決済銀行）の総支配人が「各国の中央銀行や金融当局に対し」「消費者や投資家の保護するための備えが必要」との見解を示し[16]，G20でも「仮想通貨の国際的な規制」の提案見通しが出ている[17]。

しかし投機的な動きを除けば，仮想通貨の登場の歴史的意義は大きく，改良の動きもある上に，ブロックチェーンの登場意義は更に大きい。適切に付き合えるような教育が求められる。

8 http : //diamond.jp/articles/-/158689参照。（accessed on 2018. 02. 08）

9 https : //toushi-fan.com/crypto-lisk/参照。（accessed on 2018. 02. 08）

10 http : //story-is-king.com/post-9809参照。（accessed on 2018. 02. 08）

11 https : //hikaruya.com/tipnem 参照。（accessed on 2018. 02. 08）

12 https : //doi.org/10.1073/pnas.1722031115参照。（accessed on 2018. 02. 08）

13 https : //www.houdoukyoku.jp/posts/24828参照。（accessed on 2018. 02. 08）

14 http : //ur0.work/IrSi 参照。（accessed on 2018. 02. 08）

15 http : //ur0.work/IrQL 参照。（accessed on 2018. 02. 08）

16 http : //ur0.work/IrQX 参照。（accessed on 2018. 02. 08）

17 http : //ur0.work/IrR8参照。（accessed on 2018. 02. 08）