通貨の将来と仮想通貨の意義
～デジタル化とブロックチェーンがもたらすもの～

財政金融委員会調査室　小野　伸一

１．はじめに－仮想通貨法の成立

2016 年の通常国会（第 190 回国会）において資金決済法が改正され、ビットコインをはじめとする仮想通貨についての規定が盛り込まれた。これは「仮想通貨法」とも呼ばれており、2017 年４月１日から施行されている。マネーロンダリング・テロ資金供与規制や利用者保護規制などの観点から仮想通貨交換業者（取引所など）に登録制が導入され、仮想通貨のソフトインフラ整備が本格化した。また同年７月１日からは、仮想通貨の取引（円とビットコインの交換など）に係る消費税が非課税となった。仮想通貨はビットコインの他にもイー

サリアムをはじめ数多く存在し、ウェブサイト情報[1]では850種類以上に達している。

仮想通貨はインターネット上のデジタルな無記名の資産であり、広義の金融資産ともいえるが、金融商品取引法上の金融商品には該当しない。「仮想」通貨というと何か現実のものではない語感があるが、原語はcryptocurrency（暗号通貨）であり、円やドルなどの法定通貨とは全く異なった暗号技術を用いて創造されるものの、主要なものは法定通貨と交換可能であり、実際に通用する支払手段であることに変わりはない。そして、何よりも仮想通貨はブロックチェーンという経済社会に大きなインパクトを及ぼし得るイノベーションがもとになっているところに特徴がある[2]。

一部の諸外国では既に取引所の免許制・登録制などが導入されており、我が国でも仮想通貨法で体制整備に踏み出したことから、今後さらに普及していく可能性がある。以上を踏まえ、本稿ではまずイントロダクションとして通貨の機能と現状に触れ、通貨がインターネット化、スマホ化しつつあることを述べる。次にビットコインをはじめとする仮想通貨とブロックチェーンの概要、価値と価格の考え方などについて指摘し、最後に経済のデジタル化が進展する中での通貨の将来について私見を述べたい[3]。

２．通貨の機能と現状－スマホ化の時代

通貨（貨幣）の機能については、従来から価値の尺度、交換手段、価値（富）の保蔵手段の３つが挙げられている。歴史的にみれば、貝殻や穀物、家畜など

---

[1] https://coinmarketcap.com/。なお、本稿では多くのウェブサイトを参照しており、一部のＵＲＬを脚注などに記載しているが、サイトによって情報（データ）に差異もあることをお断りしておきたい。ＵＲＬは特に断りのない限り2017年８月末現在であり、１ドル110円で換算している。

[2] 本稿はブロックチェーンを画期的なイノベーションとみる立場から記述している。ＩＴ革命をリードした基本的なイノベーションであるインターネット、ＰＣ（パソコン、タブレット）、スマートフォンはいずれも不特定多数による非階層的なネットワークに価値を見出しており、ブロックチェーンもこの延長線上にある。仮想通貨は「お金のインターネット」（Internet of Money）といわれることもあるが、筆者には「ブロックチェーン通貨」という表現がしっくりくるように思われる。後述するように（７．参照）中央銀行においても法定通貨のデジタル化が検討されているが、ブロックチェーン上で発行される場合には概念上、ブロックチェーン通貨になる。

[3] 本稿は筆者の個人的見解を述べたものであり所属する組織とは無関係である。また、本稿は仮想通貨の可能性やリスクなどに言及しているが、投資を行う場合の判断材料の提供を目的とするものではないことをお断りしたい。

の物品貨幣から出発し、金や銀などの金属貨幣を経て広く紙幣が用いられるようになった。通貨は国家による保証がないと成立しないと思われがちであるが、米国でも南北戦争まではいわゆる民間貨幣が流通していた。何が通貨かを説明する最大のポイントは一般的受容性であるといってよく[4]、その時代時代で様々な通貨が受け入れられてきた。

上述の通貨にはいずれも物理的な形があるが、形がなければ機能を満たさないわけではない。金融機関の要求払預金、すなわち預金通貨はそれ自体、目にみえるものではないし、ＩＴ化の進展で登場した電子マネーやデジタル通貨も同様である。今日では、現金を持ち歩かなくてもクレジットカードで支払いができるようになり、買い物をすれば即時に預金から引き落とされるデビットカードも使われるようになってきた。諸外国ではクレジットカードよりデビットカードの方が一般的な国も多いが、いずれにせよ通貨のカード化の時代が到来している。

さらに今日では、プリペイド型やポストペイ型の電子マネーが登場し、クレジットカードやデビットカードのモバイル決済を含め、スマートフォンでの支払いも次第に浸透してきた。我が国ではまだ定着しているとはいえない状況であるが[5]、ケニアなどサブサハラ・アフリカ地域（５．（２）②参照）や中国をはじめとする諸外国での普及には目を見張るものがあり、通貨のスマホ化の時代が到来しようとしている[6]。そしてこのような通貨のスマホ化をさらに推し進める可能性をもった存在が仮想通貨である。

３．仮想通貨の特徴

仮想通貨はビットコインを嚆矢とする。リーマンショック後の 2010 年頃に普及しはじめ、紆余曲折がありながらも次第に浸透していく一方、様々な仮想

---

[4] 館・浜田（1972）では、「われわれが普通に貨幣を貨幣として受け取るのは、それが法貨だということが念頭にあるからではなく、やはり一般的受容性を持つものだということに基づいて受け取るのだと考える方が、より現実に即した考え方である」と述べられており、本稿もこのような立場から記述している。

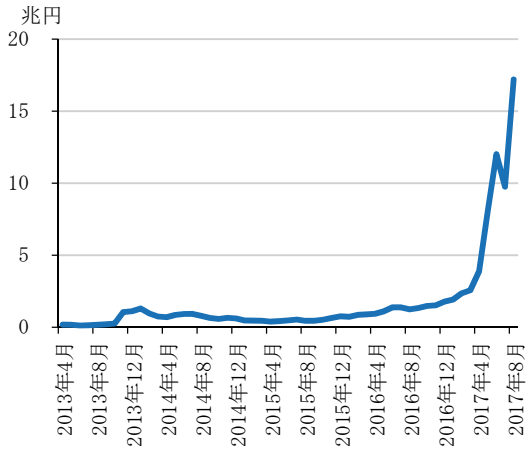
[5] https://www.boj.or.jp/research/brp/psr/data/psrb170620a.pdf

[6] 通貨のスマホ化という意味では我が国より中国の方がはるかに進んでいる。これは大手ＩＴ関連企業アリババやテンセントが提供するモバイル決済（アリペイ、ウィーチャットマネー）の存在が大きく、零細な商店までＱＲコードによるモバイル決済が常態になっている。また、欧州においても近年、「N26」というドイツ・ベルリンのフィンテックベンチャー企業が開発したモバイルバンク（スマホ銀行）が急速に普及しているようである。一方、我が国のスマートフォン保有率をみると、年齢による格差が大きく、20 代、30 代は 9 割を超えているが高齢になるほど低下し、60 代は 33.4%、70 代は 13.1%、80 代以降は 3.3%となっている（2016 年総務省調査。http://www.soumu.go.jp/johotsusintokei/statistics/data/170608_1.pdf）。

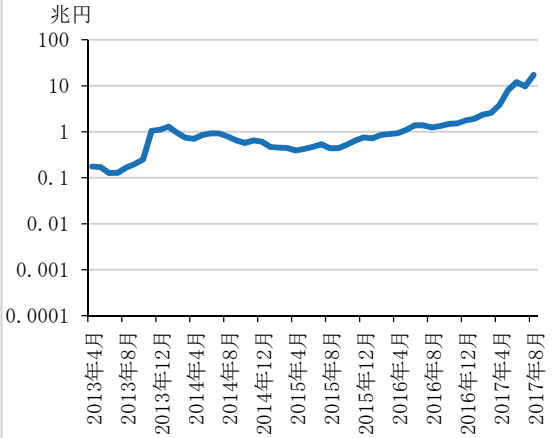
通貨がＩＣＯ（株式のＩＰＯに相当するもの。５．（１）参照）により出現し種類が増加していった。2017 年８月末現在、仮想通貨全体の市場規模は 17 兆円に達し（図表１－１、１－２）、ビットコイン、イーサリアムはそれぞれ８兆円、４兆円、ビットコイン・キャッシュ、リップル、ライトコイン、ネム、ダッシュ、アイオータ、モネロ、ネオはそれぞれ１兆円超～1,000 億円超に達している。

ここではビットコイン、イーサリアムの概要について述べるとともに[7]、仮想通貨を支えるブロックチェーン技術の特徴を指摘する。後述するようにブロックチェーンにも様々なタイプがあるが（３．（１）②参照）、その代表はビットコインで使われているような、不特定多数の人々が分散型台帳を共有することで改ざんなどの不正を不可能にしているパブリックなブロックチェーンである。

図表１－１　仮想通貨市場規模



図表１－２　仮想通貨市場規模（対数目盛）



（出所）https://coinmarketcap.com/より作成

（１）ビットコインとブロックチェーン

①ビットコインの誕生と特徴

ビットコインはリーマンショック直後の 2008 年 10 月、「サトシ・ナカモト」氏がネット上に公開した論文[8]において構想が示され、2010 年頃から普及しはじめた。同氏が日本人かどうかは諸説があり、今日でも判然としていない。当初は１BTC（単位としてのビットコインを BTC と記述する[9]）が 10 円に満たなかったが、最近では 50 万円に達することもあり（図表２－１、２－２）、５万

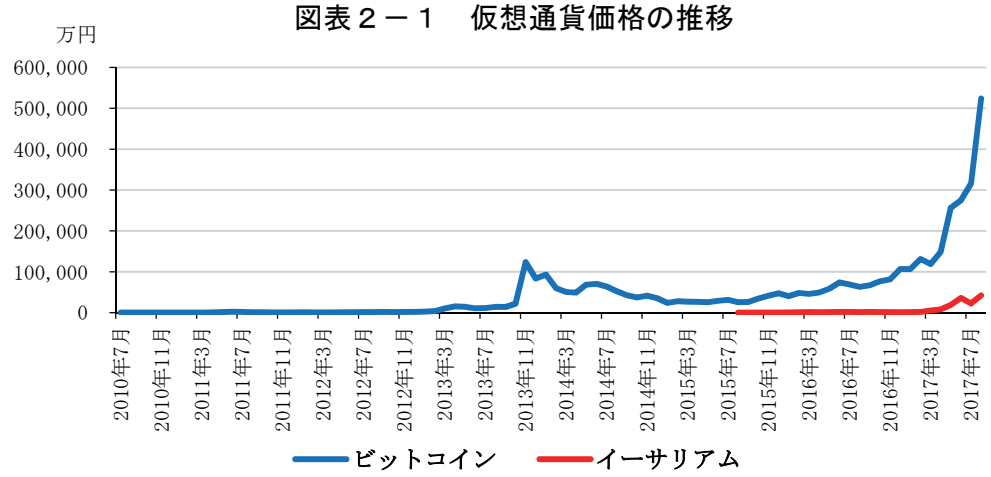
[7] リップル及び市場規模 10 位までの仮想通貨について補遺１、補遺２参照。

[8] https://bitcoin.org/bitcoin.pdf。これはビットコインのホワイトペーパー（説明書）でもある。

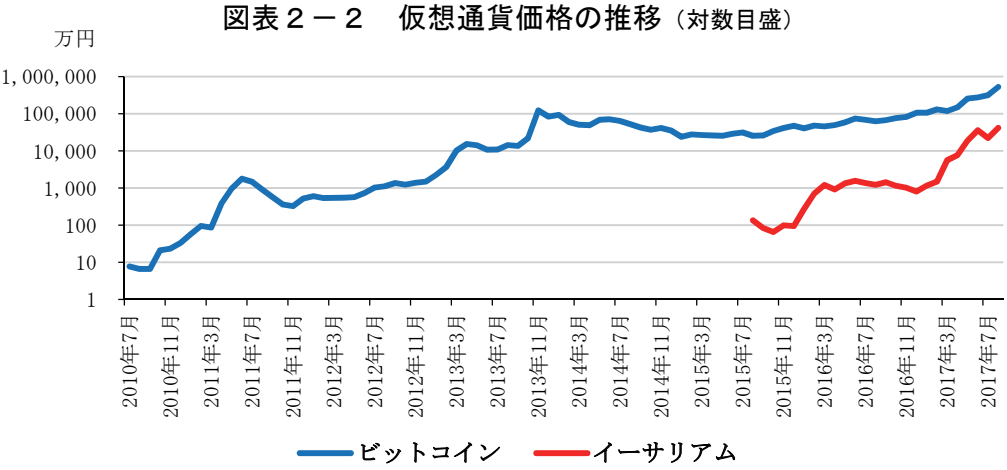
[9] ビットコインの最小単位は１億分の１BTC で、これは発明者にちなんで１サトシ（Satoshi）と呼ばれている。

倍の上昇率である。なお、2017 年９月には中国の仮想通貨取引所の閉鎖報道があり価格が乱高下しているが、これについては後述する（５．（２）①参照）。

図表２－１　仮想通貨価格の推移



図表２－２　仮想通貨価格の推移（対数目盛）



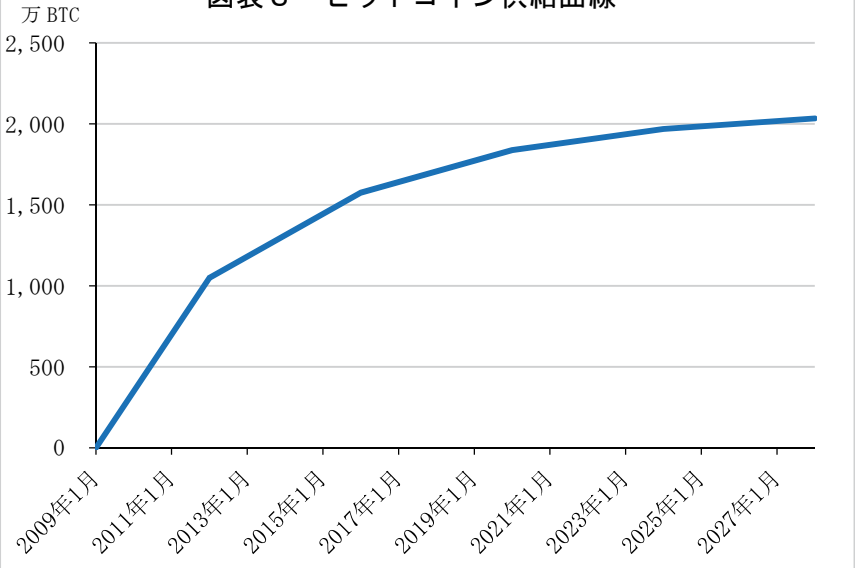
（出所）https://coinmarketcap.com/より作成

仮想通貨の供給メカニズムは法定通貨とは異なり、当初、仮想通貨の開発者などに付与されたり、ＩＣＯ時に資金提供者に対価として供与されたり、あるいは取引の信頼性を保証するためのマイニング（採掘。１．（１）②参照）と呼ばれる活動に対する報酬として付与されたりしている[10]。ビットコインの場合には総発行量はあらかじめ 2,100 万 BTC と定められており、これを超えることはない[11]。マイニングに対する報酬としてのビットコインは指数関数的に減少していき、約４年毎（21 万ブロック毎）に２分の１になる。当初は１ブロック

[10] ＩＣＯはビットコインについては行われていない。
[11] 多くの仮想通貨で発行上限が定められているが、イーサリアムのように明確になっていないものもある。

当たり 50BTC であったが、2012 年 11 月に 25BTC、2016 年 7 月に 12.5BTC となった。これによりビットコインの発行は 2140 年頃に 2,100 万 BTC となり、これ以上発行されなくなる（図表３）。2017 年８月末現在の発行高は 1,654 万 BTC である[12]。将来、マイナー（採掘者）は報酬としてビットコインを受け取ることができなくなっても、取引手数料[13]が収入として残ることから、マイニングひいてはブロックチェーンの維持に特段の問題はないとされるが、手数料のみでマイニングのインセンティブが維持できるかどうかについては疑問視する見方もある。

図表３　ビットコイン供給曲線



（出所）筆者作成

ビットコインのようなデジタル通貨は、インターネットというサイバー空間上の存在であり、サイバー攻撃に対するセキュリティ対策が不可欠であることから、1970 年代以降米国を中心に開発されてきた暗号技術が用いられている[14]。乱数を発生させてつくられた個人の暗証番号（秘密鍵といわれる）を、楕円曲線といわれる曲線を用いて数学的に変換することで公開鍵がつくられ、さらにこれをハッシュ関数といわれる、複雑なデータのインプットを要約されたアウトプット（ハッシュ値）に変換する関数を用いて口座番号（アドレス）がつく

[12] http://coinmarketcap.com/currencies/bitcoin/
[13] https://bitinfocharts.com/bitcoin/によれば、１取引当たりの手数料は平均値で 6.9 ドル、中央値で 4.2 ドルである。
[14] むしろ暗号技術の発達がビットコインのような暗号通貨を成立せしめたといった方がよいのかもしれない。

られる。これらの変換は不可逆であり、公開鍵から秘密鍵を知ることや、アドレスから公開鍵を知ることはできないため[15]、公開鍵やアドレスが公開されても（厳重に管理する限り）秘密鍵は他者に知られることはない。ちなみに秘密鍵、公開鍵、アドレスはいずれも数字とアルファベットの混在列（公開鍵は２次元（x, y）の形）で示され、個人を特定することはできない。すなわちビットコインには匿名性がある。

ビットコインの送金[16]は、秘密鍵で電子署名された送金情報をネットワーク上で流し、これをネットワークに参加している「ノード」が公開鍵で確認することにより行われる[17]。ノードとは仮想通貨のコンピュータ・ネットワーク上で他者の送金決済の承認を行う節点であり、要はこのような承認行為を行う意思を持ってネットワークに参加しているコンピュータのことである。2017 年８月末現在、世界で 9,000 超存在しており、漸増傾向にある[18]。ちなみにビットコインの送金というのは、分散型の台帳上にそのデータが記録され、送金者の残高が減少し受領者の残高が増加することを意味しており、ビットコインが物理的に移動するわけではない。

一般に、仮想通貨の売買は取引所を介して行われる場合が多い。仮想通貨と同様、取引所もまたネット上の存在であり、2017 年８月末現在で活動している取引所は我が国では 10 を超え、世界では 100 を超えている[19]。今日では、主要国においては免許制・登録制となって規制されている場合も多いが、株式売買の取引所と比較すれば小規模で分散している印象があり、特に小規模な取引所では十分な管理を行うことが可能かどうか課題もあるように思われる。取引所は仮想通貨の将来を考える上で重要なプレーヤーであるが、証券取引所と比較すれば必ずしも情報公開が十分ではない印象もあり、アカウンタビリティの向上が期待される。

ビットコインについて述べる上で避けて通れない出来事として、我が国の取

---

[15] コンピュータの計算能力が飛躍的に向上したり、量子コンピュータが実用化されれば解読されるという指摘もあるが、その時は暗号技術もさらにその先へと進歩しているのではないか。

[16] https://bitinfocharts.com/bitcoin/によれば、1 取引当たりの金額は平均値で 5.9BTC、中央値で 0.16BTC である。

[17] 公開鍵を用いることで、電子署名が同一者の秘密鍵による署名かどうかはわかるが、電子署名から秘密鍵自体を知ることはできない。これも暗号技術である。

[18] https://coin.dance/nodes、https://bitnodes.21.co/など。後者によればノードの所在地は欧米が多く、１位米国、２位ドイツ、３位フランスで我が国は 12 位である。

[19] https://www.coinhills.com/market/exchange/。我が国の取引所は必ずしも網羅されていないようである。

引所におけるビットコインの消失事件（マウント・ゴックス事件）がある。2014年２月、東京を本拠地とし一時は世界最大の取引所であったマウント・ゴックスが突然ビットコインの払い戻しを停止し、同月、民事再生法を申請して経営破綻した。2015年８月にはマルク・カルプレスＣＥＯが逮捕され（私電磁的記録不正作出・同供用、業務上横領容疑）、現在、東京地裁で公判中である。

検察側は同ＣＥＯが顧客のビットコインを横領し、残高を水増しするとともに不正に隠蔽したと指摘する一方、被告側はハッキングの被害にあったと主張している。報道によれば、ハッキングを行ったのはブルガリアの仮想通貨取引所BTC-eの関係者とされるが、仮にハッキングがあったとしても、まず問われるべきはそれを許した取引所の管理体制の甘さであろう。なお、本事件によりビットコインの信頼性が損なわれたという報道もみられたが、現金が横領されたり盗まれても現金自体に罪はないのと同様、ビットコイン自体に罪があるわけではない。

②ブロックチェーンとは何か

（マイニングの機能と意義）

ビットコインの特徴は何といってもブロックチェーン、すなわち分散型台帳をつくる技術にある。法定通貨のように物理的に存在する場合には、偽札など偽造を如何に防ぐかが大きな課題となるが、仮想通貨のようなデジタル通貨においては、二重支払（同時支払）のような改ざん行為を如何に防ぐかが大きな課題となる。

ブロックチェーンの信頼性を検証する作業はプルーフ・オブ・ワーク（ＰｏＷ）といわれ、各ノード（マイナー）がひとかたまりの取引ブロック毎に約10分かけて複雑な計算、いわゆるマイニングを行うことで承認される[20]。そして、このプロセスが繰り返されて出来上がったブロックがチェーン（鎖）のように連なることでオープンな台帳、すなわちブロックチェーンがつくられる[21]。マイナーは他者と計算力を競い、最も速く条件を満たす結果を出したマイナーが報酬としてビットコインを受け取ることができる。ただし、検証されたブロック

[20] 具体的には、ハッシュ関数による計算を一定の条件を満たす結果（ハッシュ値）がでるまで繰り返し行う。

[21] ビットコインの１ブロックのマイニングが 10 分ということの意味は、マイニング競争が無条件に 10 分以内で行われるということではなく、10 分で競争が終了して勝者が生まれるように計算の前提が調整される仕組みになっているということである。これによりマイニング能力が向上してもブロックが平均して 10 分に１つずつ増えていくこととなる。

が承認されるためには、参加しているノードの総計算能力の過半数による承認が必要である[22]。

コンピュータで膨大な計算（ＰｏＷ）を行うことがなぜ不正防止に役立つかといえば、多大なコストをかけて計算を行わなければ報酬としてのビットコインを獲得できないという仕組みが不正取引の抑止力となる[23]からである[24]。マイニング能力がシステム全体の過半（50%超）を占める不正なマイナーが現れ、不正行為を行ったブロックを分岐させ正しいブロックとして承認しマイニングし続けてしまえば不正は防止できないようにも思われるが、取引規模が拡大しマイニングコストも増大する中で過半を握るということは考えにくいことである[25]。

１ブロックに含まれる取引記録数はバラツキがあるが 1,000～2,000 前後、全ブロック数は 2017 年８月末現在で約 48 万である。これをネット上に分散するノードが共有、いわば相互監視することで改ざんが防止され、信頼性が確保される。個々のノードがネット上でつながり、情報交換を行う仕組みはＰ２Ｐ（peer-to-peer）方式と呼ばれ、従来のクライアント・サーバ方式のコンピュータ・システムの対極をなすものである。

ビットコインはスクリプトといわれるプログラミング言語が用いられ、ソースコードは公開されており（オープンソース）、誰でも確認することができ提案

---

[22] 承認が同時に行われるなど、何らかの要因でブロックチェーンが分岐する可能性もゼロではないが、ルール上、最も長いチェーンが正しいチェーンとなる。承認が６回積み上げられればほぼ安全とされている。

[23] 例えば、ある不正行為者が二重支払など改ざんされた取引を含むブロックをつくっても、それが承認されて報酬を得るためには計算競争に勝つ必要があり、このためには多大なコストをかけて計算能力を高めなければならないことから、改ざんは割に合わないものとなる。

[24] これは過去のブロックについても同様である。過去に生成されたブロックを改ざんすれば、（各ブロックではデータをハッシュ関数で圧縮・要約したハッシュ値が算出され、これが次のブロックに申し送りされているので）その後に続く全てのブロックについて計算し直さなければ整合性がとれなくなり、これは膨大なコストを要することから事実上不可能となる。

[25] 仮に不正なマイナーがマイニング能力の過半を握ったとしても、ブロックチェーンの信頼性は著しく低下し、ビットコインの価値も大きく毀損してしまうであろうから、何よりも当該マイナー自身が最大の不利益を被る結果となってしまう。なお、不正なマイナーがマイニング能力の過半を握る事態に対しては、コミュニティサイドでプロトコル（コンピュータ同士のやりとりのルール）を変更することによっても対処できるといわれる。ちなみにコミュニティとは仮想通貨のルールの設定や修正などに関わる人々のグループで、ビットコインやイーサリアムなどでは活発に活動しているが、意見の対立から中核的なメンバーが離脱したりハードフォーク（３．（１）③参照）が生ずることもある。日本人メンバーは少ないようであるが、いずれにせよ仮想通貨の理解はコミュニティの主なメンバーの言動をフォローすることなしには難しい印象がある（テクニカルな内容も多く容易ではないが）。

も可能であるが、採択されるためにはコミュニティの支持が必要である。取引もブロックチェーンの形で全てが公開されており、誰でもネット上で確認することができる[26]。常時、世界中の不特定多数の人々の目にさらされ、マイニングという人為的に操作できない純粋な競争原理が貫徹しているからこそ信頼性のあるネットワーク・システムが構築できているのであり、ここに「打たれ強い」ビットコインの神髄がある。一般的受容性がなくなれば消えていくであろうが、そうでない限り人為的になくすことはできないのがビットコインである[27]。

（ブロックチェーンの意義と種類）

ブロックチェーン技術は、様々な経済社会活動の信頼性・効率性を追求する手段としてその適用領域・分野は広く、後述するように金融や財・サービス、流通・不動産、エネルギーなど様々な市場や公的セクターが対象となり得る（４．（１）④参照）。また、ブロックチェーンは不特定多数の承認により運用されるパブリック型が基本であるが、企業間の連携で活用したり（コンソーシアム型）、一企業・組織が集権的に業務・履歴管理を行う場合に活用すること（プライベート型）も不可能ではない。コンソーシアム型やプライベート型では、ブロックチェーンのネットワークは限定的なノード（管理者）だけで構成され、ビットコインの不特定多数によるネットワークとは本質的に異なったものとなるが[28]（図表４）、効果としては、従来の中央制御型のデータベースがブロックチェーンに置き換えられることによるコストダウン、業務プロセスのトレースやチェックの容易化などが想定される。

コンソーシアム型やプライベート型のように信頼がおける（はずである）参加者だけで構成されるブロックチェーンの場合には、不正な運用をチェックするプルーフ・オブ・ワーク（ＰｏＷ）を厳格に適用しなくてもよいのではないかという考え方が生まれ[29]、ビットコインのような、ブロックチェーンを機能さ

---

[26] https://blockchain.info/で全てのブロックの取引内容を確認することができる。

[27] 米国や中国、ロシアなどには影響力の行使（コントロール）を狙う人々が存在すると報道されているが、取引所などに対する規制の形で行われるであろう（ビットコイン自体＝コミュニティのコントロールは不可能である）。

[28] コンソーシアム型やプライベート型は特定のノードだけで構成されることから、パーミッション型（permissioned）ともいわれ、一例として我が国企業も参加しているハイパーレッジャー・ファブリック（Hyperledger Fabric）がある。これはイーサリアムなどとは異なり、仮想通貨（トークン）を含まないブロックチェーンの管理運営に絞ったプロジェクトである。

[29] ただし、パブリック型以外のブロックチェーンにパブリック型と同様の価値が認められるかどうか、パブリック型と同レベルの信頼性を維持できるかどうかについては懐疑的な見方もあ

せる「燃料」の役割を果たす存在（トークン[30]と呼ばれる）も必ずしも必要不可欠なものではなくなる。ブロックチェーンはもともとビットコインを成立させるために考案されたものであったが、ビットコインから離れて独り立ちし、多様に成長していくことで経済社会の様々な局面で適用可能なものとなった。そのポテンシャルが極めて大きいことは疑う余地がないと思われる。

図表４　ブロックチェーンの類型

	パブリック型	コンソーシアム型	プライベート型
	非パーミッション型	パーミッション型	
参加者（ノード）	不特定多数 （管理者なし）	信頼できる者・選ばれた者 （＝管理者）	1組織（＝管理者）
取引者	不特定多数	制度設計次第（オープンにも特定者のみにもできる）	制度設計次第 （通常は特定者）
ネットワークへのアクセス	不特定多数	制度設計次第（オープンにも特定者のみにもできる）	制度設計次第 （通常は特定者）
合意形成メカニズム	不特定多数によるマイニング	許可されたノードによる合意形成	自ら承認
コンセンサスアルゴリズム	PoW、PoSなど	BFT（Byzantine Fault Tolerance）など （→ノード数が既知で不正コード数に上限があるなどの条件下で機能するアルゴリズム）	
主な用途	仮想通貨	ビジネス一般	各種組織

（出所）筆者作成

③ハードフォークとソフトフォーク

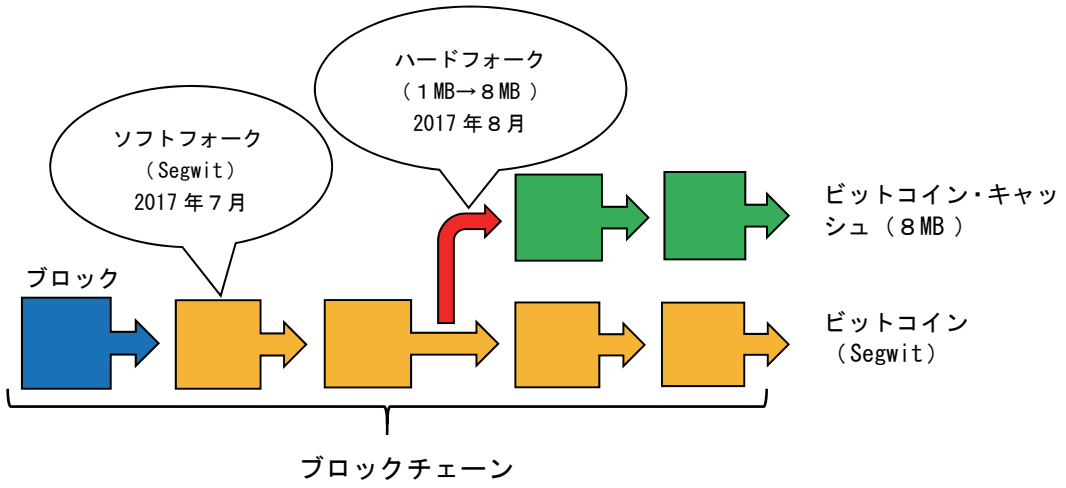
仮想通貨の世界でしばしば登場する用語にハードフォークとソフトフォークがある。ハードフォークはそれ以前のルールと互換性がない修正であり、以前のルールは使えなくなる。これに対してソフトフォークは互換性のある修正であり、以前のルールは引き続き使用でき、しばしば新たなルールも追加される。イーサリアムでは後述するように2016年にハードフォークによる分岐が生じ、新たな仮想通貨が誕生することとなった（３.（２）③参照）。最近では2017年７月、ビットコインにおいてSegwit（Segregated Witness）といわれる、署名を分離することでブロックの容量を実質的に増大させるソフトフォークが成立し、同年８月から実施された。また同じ８月には、中国のマイニングプール

る。

[30] トークンとは、ブロックチェーン上でつくられるデジタルな資産（コインのようなもの）を意味しており、報酬としても使われる。

（ViaBTC）が主導してブロックの容量を１MB から８MB に引き上げるハードフォークが行われ、「ビットコイン・キャッシュ」という仮想通貨がビットコインから分岐して成立することとなった（図表５）。さらに 2017 年 11 月には、ブロックの容量を２MB へ増大させるハードフォークが行われるという情報がある（行われない可能性もある）。

図表５　ビットコインのソフトフォークとハードフォーク



（出所）筆者作成

このようなビットコインの動きは、主に、同コインに内在するスケーラビリティ問題、すなわち１ブロックの承認に 10 分かかることに由来する取引処理能力の限界を如何に緩和するかという問題への対応として生じている。Segwit が成立したことで、取引の一部をオフチェーン化し、取引の増大に対応するライトニング・ネットワーク[31]といわれる手法などの実装も容易になるとされている。

いずれにせよ、ビットコインは自律的、分権的な通貨でありコミュニティには様々な意見があることや、近年はマイニングプールが存在感を増し影響力を行使しようとしていることなどから、今後とも分岐する可能性は常に存在している。これは後述するビットコインのボラティリティ（価格の変動。４．（３）参照）を高める一因ともなっているが、逆にいえばそこに投資機会も存在している。ハードフォークによる分岐を「分裂危機」などと煽るような論調もみられるが、ユーザーにとってはむしろ選択肢の拡大につながる面もあり（選択さ

[31] 例えばA→B→C→Dという送金をブロックチェーン上ではA→Dとのみ記録することで記録量を抑制し、手数料も削減することができる。このようにブロックチェーン（レイヤー）に新たなレイヤーを重ねる手法は「レイヤー２」「セカンドレイヤー」といわれる。

れなければ消えていくだけである)、現時点ではこれが仮想通貨の常態であるとさえいえるように思われる。

（２）イーサリアム

①プラットフォームとしてのイーサリアムとトークンとしてのイーサ

（機能と役割）

イーサリアムは 2013 年、ロシア生まれでカナダ移民の Vitalik Buterin 氏によって構想が示され、2014 年から運用が始まり、2015 年に正式に立ち上げられた。その大きな特徴は、ビットコインでは取引記録の管理だけが行われるのに対し、イーサリアムでは様々な情報を書き込んだプログラムをブロックチェーン上で自動的に作動させたり、プログラムを含む様々なアプリケーション（ソフトウェア）を作動させたりできることである[32]。一度書き込まれれば改ざんできないことはビットコインと同様である。プログラムの自動的な作動は「スマートコントラクト」といわれ、イーサリアムはスマートコントラクトの基盤であるとしばしば表現されるが、コントラクトは日本語の「契約」と必ずしも同義ではなく、一定の条件が満たされれば特定の行為が行われるなど自動的にプログラムが執行されることを意味している。さらにイーサリアムは「様々なアプリケーションを動かすことができる汎用性の高い、オープンで分散型のプラットフォーム（実行環境)」であるともいわれる。

イーサリアムは Solidity というプログラミング言語が使われ、どのようなプログラムでも書くことができ、これは「チューリング完全」といわれる。チューリング完全であれば無限ループ、すなわちいつまでも処理が終わらず止められない不都合なプログラムが生じてしまうこともあるが、イーサリアムでは、プログラムを実行するために燃料（ガス）を必要とし、燃料が切れればプログラムの実行がストップすることでこのような欠点をクリアーしている[33]。この燃料はイーサ（Ether）と呼ばれている。

イーサリアムはそれ自体が仮想通貨であるように思われがちであるが、実際には、イーサがイーサリアムというアプリケーション・プラットフォームを作

---

[32] ビットコインで使用されているブロックチェーン技術などを通貨以外の用途へ応用したり、様々な価値のブロックチェーン上での流通を目指すプロジェクトは「ビットコイン 2.0」と呼ばれており、イーサリアムもその１つである。

[33] 逆にビットコインのスクリプト言語はチューリング不完全でプログラミングに制限があるが、無限ループが生ずることはない。

動させる燃料、換言すればプラットフォームの利用料（トークン）となり、プログラムのアドレスにイーサを送金することでプログラムが起動する。プログラムのコードがオープンソースであることはビットコインと同様である。

イーサの当初の発行額は7,200万ETHであり、このうち6,000万ETHが2014年のＩＣＯにおける購入者に供与され、1,200万ETHが開発者や初期の貢献者に提供された。マイナーへの付与を含め、2017年８月末時点での発行額は9,436万ETHとなっている[34]。価格は2017年８月末現在で４万円に達しており、当初は100円前後であったから、約２年で400倍の上昇率である（図表２－１、２－２）。

（ブロックチェーン）

イーサリアムにおいても、マイニングによりトークン（イーサ）が提供される手法はビットコインと同様であり、新たなブロックのマイナーに５ETHが付与される。一方、１ブロックの完成時間はビットコインより短く、平均して15～17秒程度となっている。マイニングコストとともに、プログラムの執行やネットワークの保守などコンピュータ関連費用も付与されるイーサによって賄われるが、後述するようにイーサの価格は必ずしもこのようなコストだけから説明できるわけではない。これはビットコインも同様である（４．（１）（２）参照）。

なお、開発者が公表した情報によれば、イーサリアムのブロック承認の方法は、ビットコインのような計算能力・スピードによる承認（ＰｏＷ）から、プルーフ・オブ・ステーク（ＰｏＳ）といわれるトークンの保有量に基づく承認へと移行することが予定されている[35]。2018年にも実施される可能性があるとされているが、スケジュールは必ずしも明確ではない。

全体にイーサリアムは、その基本においてはビットコイン同様、自律・分散型で管理者がいないブロックチェーンに基づくシステムではあるが、ビットコインほど分権的ではなく、より開発者（Buterin氏）の意向を踏まえた運営が行われているようにも見受けられる。これは後述するTheDAO事件への対応にも現れている（３．（２）③参照）。

②イーサリアムの機能

---

[34] http://coinmarketcap.com/currencies/ethereum/

[35] ＰｏＷやＰｏＳのようなブロックを承認するアルゴリズムのことを、一般にコンセンサスアルゴリズムと呼んでいる。

（ブロックチェーンとイーサリアム）

イーサリアムは汎用性のあるプラットフォームであり、これを活用した様々なプロジェクトが立ち上がり、ＩＣＯも行われている。例えば、オーガー(Augur、トークン：REP）というプロジェクトは、参加者が様々な未来予測を行い、これが正しい場合に報酬としてREPが付与されるというものであり、イーサリアムのブロックチェーン上にルールがスマートコントラクトで記録され運用される[36]。このような仮想通貨は、ビットコインの代替的なコインという意味で、アルトコイン（Alternative Coinの略称）と呼ばれることがある[37]。近時のＩＣＯで立ち上がったアルトコインには、このようなイーサリアム上でつくられたトークンの形になっているものがかなり存在しており、もともとイーサリアムはこのような利用を想定してつくられている。

イーサリアムに基づく自動的・自律的なプログラムは、経済社会の様々な局面で活用が可能と考えられる。我が国を含む世界の大手企業は、イーサリアムとそのブロックチェーンのビジネスへの活用に連携して取り組む企業連合（Enterprise Ethereum Alliance：ＥＥＡといわれる）を立ち上げており、Ｒ＆Ｄに取り組んでいる。また、外国貿易・金融分野においては、イーサリアムをベースにしたブロックチェーン上で電子化された信用状（Ｌ/Ｃ）や保険証券を流通させる実証実験が行われており、業務の効率化に貢献することが確認されている。

（Dapps、ＤＡＯとイーサリアム）

イーサリアムは近時、様々な分散型のアプリケーション（Decentralized Applications：Dapps といわれる）のプラットフォームとしての機能を果たすことや、イーサを燃料として自律的・分権的に機能し続ける組織体（Decentralized Autonomous Organization：ＤＡＯといわれる）を動かすことが強調されるようになっている。ＤＡＯの一例として後述するTheDAOがあるが（３.（２）

---

[36] オーガーは保険や、天候デリバティブなどの金融デリバティブ、さらにギャンブル機能などを併せ持つとされる。ＩＣＯの成功例の１つとの見方がある一方で、今後の発展可能性に疑問を呈する向きもある。

[37] ビットコインについても、取引データが書き込まれていないスペースに株式やクーポン、不動産や動産などの様々な情報を書き込むことができる。これは、ビットコインに通貨以外の資産としての「色」を付けるという意味で「カラードコイン」と呼ばれている。また、ビットコインなどのブロックチェーンに他のブロックチェーンを紐付け、別の仮想通貨をつくってやりとりしたり、通貨以外の機能を持たせたりすることがあり、「サイドチェーン」と呼ばれている。

③参照)、これはプログラムに欠陥があったためハッキングの被害にあい、目的を達することができなかった。また、必ずしもイーサリアムをプラットフォームとして利用する場合に限られるわけではないが、多くのプロジェクトがＩＣＯにより多額の資金獲得に成功している割には結果が伴っていないという批判もある（５．（１）参照)。

他方で、イーサリアムなどのプラットフォームが広く経済社会に普及していくなら、組織と契約（コントラクト）のバランスに変化が生じる可能性も生ずる。かつてノーベル経済学賞を受賞したロナルド・Ｈ・コースは、1937 年の論文（『企業・経済・法』所収の「企業の本質」）において、市場も企業も資源配分の役割を担うものであるが、いずれもコストがかかり、市場取引コストより組織内取引コストの方が小さければ組織内取引、すなわち企業を利用することになると指摘して企業の成立を理論的に説明した。これは、イーサリアム型のプラットフォームの活用によりＰ２Ｐ方式を基本とする分散型組織（ＤＡＯ）が有効に機能すれば、物理的に集合する企業型の組織よりもＤＡＯが優位に立つ可能性が生ずることを意味している。もちろん実際には様々な制約条件があり一筋縄では進展しないであろうが、今後のイーサリアムの可能性の一端を示すものとして注目される。

③TheDAO 事件

イーサリアムについて述べる上で避けて通れないのが TheDAO 事件である。2016 年６月、投資ファンドを自律分散型の組織で運用するプロジェクトである TheDAO（トークン：DAO）がＩＣＯを行い、1,150 万 ETH を調達したが、コントラクトのコード上のバグを突かれてハッキングされ、投資家から預かっていた 360 万余 ETH が流出した。問題があったのはイーサリアムのプラットフォーム上でつくられ、スマートコントラクトとしてルールがブロックチェーンに記録されるプロジェクトである TheDAO 側であり、イーサリアム自体に問題があったわけではないが、イーサリアムの開発者は事態を収拾するためハードフォークを行い、ハッキングをなかったこととすべく時間をハッキング前に戻し、失われたイーサを取り戻した。一方、このようなやり方に反発した一部の技術者は従来のイーサリアムを維持し、イーサリアム・クラシック（トークン：ETC）を立ち上げたため、イーサリアムは分岐することとなった。イーサリアム・クラシックも一定の市場規模があるが（2017 年８月末現在で 11 位)、広く普及し利用されているのはイーサリアムの方である。

なお、TheDAO のトークン DAO については、ＳＥＣ（米国証券取引委員会）が

2017 年７月に報告書[38]を公表し、米国証券取引法上の有価証券であると明言した。ただし、同法上の捜査は行わないこととされている。ＳＥＣの説明によれば、ＩＣＯが行われる全てのトークンではなく、TheDAO のように収益分配を行うファンドを立ち上げる場合などに同法が適用されるということのようであるが、ブロックチェーン上の自律的・分権的組織（ＤＡＯ）であっても発行主体が存在しないとはいえず、同法の規制を逃れられないという米国政府当局の姿勢は注目される。加えてシンガポールの通貨当局も 2017 年８月、ＩＣＯで発行されるトークンに同国の金融先物法が適用される場合があることを明らかにしており[39]、今後、ＩＣＯに際しては各国の証券法制との整合性のチェックが必要となる可能性が高まっている[40]。

４．仮想通貨の価値と価格、ボラティリティ

（１）仮想通貨の価値

①価値の源泉

一口に仮想通貨といってもその性格は様々であり、①ビットコインのように通貨そのものであったり、②イーサリアムのようにプラットフォームとして機能するものであったり、さらに③プラットフォーム上の収益を生むプログラムのトークンであったりする。③の場合には、トークンの価値は将来的な収益の割引現在価値と考えればよいであろうが（このようなトークンのＩＣＯが規制されようとしていることは上述の通り）、①や②の場合の仮想通貨の価値の考え方については定説はないように思われる。ここでは筆者なりに考え方を整理してみたい。

ＢＩＳの 2015 年の報告書[41]では、仮想通貨の本源的価値（intrinsic value）はゼロであり、その価値は当該仮想通貨が他の財・サービスや法定通貨に交換されるという信頼のみに由来すると述べられている。これは、法定通貨は仮想

---

[38] https://www.sec.gov/litigation/investreport/34-81207.pdf

[39] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx

[40] 2017 年９月には、中国人民銀行（政府）が国内でのＩＣＯによる資金調達を違法なものとして禁止した（http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html）。これは収益分配を行うようなトークン以外のＩＣＯも一律に禁止するものであり、その狙いは必ずしも明確ではない（資金の国外流出への懸念やコントロール権の掌握の意図が感ぜられるが、永続的なものかどうかは不明である）。なお、ＩＣＯの質的な面については、これまで様々な問題点が指摘されてきたのは事実である（５．（１）参照）。

[41] http://www.bis.org/cpmi/publ/d137.pdf

通貨とは異なりそれ自体に本源的価値があるようにも聞こえるが、法定通貨であろうが仮想通貨であろうが通貨の本源的価値は一般的受容性に起因すると考えた方が現実に適合しているであろう。ひとたびデフォルトが発生すれば、どのような法定通貨であっても一般的受容性に問題が生ずるのは歴史の教えるところであり、同様に一般的受容性に乏しい仮想通貨も消えてなくなる運命にある。

では、仮想通貨の一般的受容性の源泉は何かといえば、私見では、①ネットワーク・システム自体の価値による部分、②法定通貨との比較による部分（インフレの程度や送金コスト、手数料などからみた利便性）、③仮想通貨が生み出す社会的便益や期待による部分に分けられる（図表６）。①はビットコインに代表される自律的、分権的でパブリックなブロックチェーン・システム自体の価値であり、これまで縷々述べてきたので、以下では②、③に焦点を合わせて指摘したい。

図表６　法定通貨・仮想通貨の一般的受容性

（注）全ての仮想通貨ではない

（出所）筆者作成

②法定通貨と比較した特徴

ビットコインに代表されるように仮想通貨の多くはインフレーションへの懸念からあらかじめ発行上限を設けたり、インフレ率が低くなるように発行高をコントロールしており、相対的にディスインフレーショナリーなものとなっている。これには、法定通貨が政策的な金融緩和によりインフレーショナリーになりがちであり、減価の懸念があることへのアンチテーゼとしての意味合いも

込められているように思われる[42]。そしてこのような仮想通貨の供給メカニズムが仮想通貨の価値（一般的受容性）を生み出しているように思われる。

またビットコインなど仮想通貨には、海外送金のコストが安く、かつ 24 時間 365 日いつでも送金可能[43]というメリットがある。我が国では、一般に銀行経由で円を送金する場合には、数千円前後の手数料と日単位の日数がかかり手続きも煩雑であるが、ビットコインであれば高くても数百円前後の手数料[44]と分単位の所要時間で済む。このような利益は誰でも享受可能であり、特に低所得で銀行口座が持てない一方で海外送金の必要性の高い海外移民や難民、出稼ぎ民などにとっては大きな利益となる可能性がある[45]。後述するように、紛争地域など治安がよくない地域の住民に対する海外からの支援や寄付などにおいても有用であろう（５．（２）②参照）。

さらに、仮想通貨には決済手数料が安いという特徴がある。我が国で決済に際して店舗側が支払う手数料は、クレジットカードで４％内外（業態などで異なる）、デビットカードではこれより若干低めと思われるが、ビットコインなら現状（店舗側が法定通貨への交換リスクを負わない前提で）１％程度であり、カードの半分以下である。

加えて仮想通貨は、海外旅行など国境をまたいで移動した際に両替の必要がないという意味で利便性があり、資産ポートフォリオの分散や金融危機などの発生に備えた資産防衛にも役立つ場合がある。後述するように、特に自国通貨に不安定性があり、高インフレやデフォルトの恐れがあるような国や地域では、仮想通貨を保有することによる資産防衛や金融アクセス改善が意義をもつ可能

---

42 ただし、ハーバード大学のケネス・Ｓ・ロゴフ教授は、ビットコインを模倣したビットコイン 2.0 や 3.0 が出現することで全体として供給量が増大する可能性があるため、懸念すべきはデフレではなくインフレであると指摘している（『現金の呪い』）。実際、ハードフォークによりビットコイン・キャッシュが立ち上がり、発行はビットコインとほぼ同数となっているが、少なくとも現時点では市場規模が小さく（ビットコインの１割強）、ビットコインほどの存在感（一般的受容性）はみられない。

43 これはゼロダウンタイムといわれる。クライアント・サーバ方式ではシステムダウンの可能性をゼロにはできないが、仮想通貨のようなネットワーク・システムでは、仮に一部のノードがサイバー攻撃を受けても全体がダウンすることはない。ビットコインのネットワークはこれまで一度も止まったことがない。

44 手数料はビットコイン価格の上昇や承認待ち取引の増加などでかなり上昇したが、Segwit の成立により、手数料算定のプロセスも改善され、低下していくことが期待される。

45 世銀の報告では、2016 年の海外送金は発展途上国向けが 47 兆円、世界全体では 63 兆円である。送金コスト（200 ドルを送金する総コスト）は 7.45%（2017 年第一四半期）であり、世銀の持続可能な開発目標の３％を大幅に上回っている。特にサブサハラ・アフリカ地域では 9.8%（同）と高率である（http://pubdocs.worldbank.org/en/992371492706371662/MigrationandDevelopmentBrief27.pdf）。

性がある（図表７）（５．（２）①参照）。

図表７　仮想通貨のプラス面とマイナス面

《プラス面》
・発行上限があり減価しにくい（価格は変動）
・ゼロダウンタイム、送金コスト・手数料が安いなどの利便性
・ボーダーレスで両替を必要としない
・ネットワークに価値あり。ブロックチェーンの普及による価値増大の期待
・低所得で銀行口座を持てなくてもスマホがあれば利用可能
・通貨危機などの際に代替通貨の機能を果たす

《マイナス面》
・ボラティリティが大きく富の保蔵機能に難あり
・現時点では利用範囲が限られ投機的需要が大
・ICO により数が増えるも質に問題あり
・犯罪に利用されたりサイバー攻撃のターゲットとなる
・秘密鍵の自己管理に手間がかかる

（出所）筆者作成

③仮想通貨の通貨発行益とコスト

一般に通貨の額面と発行コストの差は通貨発行益(シニョレッジ)といわれ、中央銀行（政府）が獲得するが、仮想通貨では通貨発行益が中央銀行に帰属しないという特徴がある。すなわち、仮想通貨の通貨発行益は、価格からマイニングコストやネットワークの維持・改善コストなどを差し引いたものと考えることができるが、これは当初からの仮想通貨の保有者（コミュニティメンバーなど付与された者）やマイニングにより仮想通貨を取得するマイナーが取得する。以下で述べるようにマイニングには一部集中化が生じており、広く不特定多数の人々に利益が及ぶわけではないものの、非公的セクターに帰属するのは興味深い点である。もちろんこれは政府・中央銀行との利益相反・対立を生む要因ともなり得るのであるが、仮想通貨の開発やＩＣＯが究極的にこのような通貨発行益の獲得を目指して行われる面があることは否定できないであろう。

ビットコインは成立当初、マイニングに必要な電気代を賄うことができるように価格（法定通貨との交換比率）が設定されたとされるが、マイニング競争は次第に激化しており、今日では相当なエネルギー投入が必要となっている。個人のＰＣによるマイニングでは能力的に太刀打ちできず、複数のマイナーがASIC（Application Specific Integrated Circuit）と呼ばれる高速計算が可能な専用チップを集積した大型コンピュータを設置・稼働させて共同採掘するマイニングプール方式がとられるようになっており、マイニングの集中化が生じ

ている[46]。過半は電力料金が安い中国にあるが、米国や、ネット環境が充実し寒冷でコンピュータの保守に好都合とされるアイスランドなどにも設立されている。マイニングの総コスト（電気代、施設・コンピュータなどハード代、人件費など）がどの程度であるかは必ずしも明らかではないが、現在、マイニングの報酬は１BTC50 万円として１ブロック（10 分）で 600 万円、年間では 3,000 億円に達していることから、有力なマイナーが利益を得ていることは間違いないと思われる。

マイニングの総コストに占める割合が最も高いのは電気代であり、マイニングは資源の無駄遣いであるとの指摘もあるが、余剰電力や水力発電など自然エネルギーの有効活用も考慮されているようである。そもそもマイニングは、ビットコインの信頼性を維持するために必要不可欠な行為であり、ビットコインの価値の源泉ともいえるものであるから、マイニングを否定することはビットコインの存在自体を否定することにつながる。画期的なイノベーションであるほどコストも大きく、社会的なコンセンサスをつくりあげることが難しいという一例であるように思われる。

④仮想通貨の社会的便益

ビットコインなどの仮想通貨が一般的に受容される背景には、開発された仮想通貨及びそれと一体的なネットワーク・システム、端的にはブロックチェーンが生み出す社会的便益への期待がある。

経産省の『ブロックチェーン技術を利用したサービスに関する国内外動向調査』（平成 27 年度）[47]によれば、我が国においてブロックチェーンがインパクトを及ぼすであろう市場規模の総計は、金融分野を除き約 67 兆円と見積もられている。具体的には、

・サプライチェーン（商品の製造・流通・販売プロセスのトレース[48]と管理など）31 兆円

・スマートコントラクト（各種契約や電力サービスの執行管理、ＩｏＴ

[46] https://blockchain.info/ja/pools。ASIC は主に中国で生産されており、2017 年８月末現在で中国のマイニングプール Antpool が全体のマイニング能力の２割弱を占めるなど、大手は中国系が多い。コミュニティには寡占化を懸念する声もあるが、2017 年８月のソフトフォーク（Segwit）はマイナーではなくユーザー（ノード）やコミュニティのメンバーがイニシアティブをとり、最終的にマイナーもこれに応ずる形で行われた。

[47] http://www.meti.go.jp/press/2016/04/20160428003/20160428003-2.pdf

[48] ブロックチェーンによる商品のトレーサビリティの向上は、経済実態のより的確な把握や統計精度の向上など、金額で表すことのできない価値の創出につながることも期待される。

（Internet of Things）管理、徴税など）20 兆円
・各種サービス（シェアリングエコノミー、デジタルコンテンツ、オークション、地域通貨、チケットサービス、ポイントサービスの管理など）15 兆円
・公的分野・医療分野（登記、特許、投票、各種届出・証明、電子カルテなど）1 兆円
などである。

金融分野では、現在のメインフレーム（大型コンピュータ）に基づく中央集権的な決済・送金システムが大きな影響を受ける可能性がある。我が国の銀行が取り扱う内国取引は１日で約 12 兆円､外為取引は 16 兆円に達しており(2016 年)、国債取引（対顧客取引）も同程度の額がある。一方、証券取引の売買高は現物市場で 760 兆円、先物やオプションなどデリバティブ市場では 2,290 兆円に上る（2016 年)。既に米国では、新興企業向け株式市場ナスダックにおいて、ブロックチェーン上で未公開株式のトークンを発行するシステム(Nasdaq Linq)の運用が始まっている。将来的には、トークンとしての株式や債券がブロックチェーン上でスマートコントラクトにより取引されたり、Ｐ２Ｐ方式で行われる分散型の取引（Decentralized Exchange：ＤＥＸといわれる）が普及して裾野が広がっていくなら、多大なインパクトが及ぶ可能性がある。

ちなみに、ブロックチェーンがもたらす社会的便益は必ずしも金銭的なものに限られないと思われる。米国の著名な経営学者であるマイケル・Ｅ・ポーターは、2011 年の論文で「共通価値の創造」（Creating Shared Value：ＣＳＶ)、すなわち企業が社会的価値を創造することを通じて競争優位を確保していくことの重要性を指摘したが、ブロックチェーンはまさにこのような共通価値（ＣＳＶ）に当たるものではないか。もちろん金銭（経済）的な面についても、ブロックチェーンの影響が及ぶであろう世界の市場規模は、経済規模が我が国の十数倍はあることから、金融分野を含めれば兆円ではなく京円単位であることは間違いない。そして仮想通貨の価格は、ブロックチェーンの導入による将来的な市場規模の拡大で生み出される価値や非金銭的な価値、期待がどの程度、仮想通貨の市場規模とリンクするか、すなわち仮想通貨の需要をもたらすかに依存するのではないかと思われる。

（２）仮想通貨の価格－期待の影響

一般に金融資産の理論的な価格は当該資産が将来的に生みだすキャッシュフローを現在価値に割り引いて計算されるが、仮想通貨の場合には、直接的には

このような将来キャッシュフローは発生しない。この意味では仮想通貨はやはり通貨に近いといえる[49]。ただし、法定通貨であればその価格である為替レートは金利や通貨供給量、物価水準（購買力平価）、経常収支をはじめとする経済のファンダメンタルズと関係するが、仮想通貨の価格も何らかの経済指標と関係するのか、あるいは独立したものであるのかは必ずしも明らかではない[50]。

ビットコインをはじめ多くの仮想通貨は供給に上限が設定されているので、価格に対しては需要が大きな影響を与えることとなる。需要には実需もあれば投資（投機的）需要もあり、実需としては送金コスト・決済手数料が安いことやその他の利便性から生ずる需要などがあるが、現在は投資の割合が高いのではないかと推測される。投資需要は人々の将来見通しの影響を受け、ブロックチェーンが社会に浸透し、仮想通貨がより広く受け入れられて価格が上昇するという期待があれば、現時点で購入する動機が生ずる。

人々の将来見通しには、仮想通貨とドルや円などの法定通貨との関係も影響を与えると思われる。既述のように、一般に法定通貨は政策的な金融緩和によって供給量が増大しインフレがつくり出されることが多いので、相対的にディスインフレーショナリーな仮想通貨の価値が上昇していく期待が生じ、需要増を生む可能性がある。

なお、強い投機的動機が市場を支配し、期待が過剰になる場合には、いわゆるバブルが発生することもあり得る。バブルというのは本来、価値を大幅に上回る価格上昇がみられる状況であるが、ビットコインの場合には現在価値を具体的に算出することが難しいことから、バブルであるかどうかの判断は容易ではない。仮に期待が期待を呼んでスパイラル的に価格が上昇する状況をバブルというなら、これまでも何度か生じていた可能性がある。1ビットコインが50万円に達する昨今の状況についてもバブルであるという指摘があり、これは仮想通貨の約17兆円（2017年８月末）という市場規模が過大であるという見方が背景にあるが、他方で市場規模はいずれ桁違いに増大するという予想もあり、将来見通しの「ボラティリティ」が非常に大きいのが仮想通貨の特徴である。

---

[49] 仮想通貨はデジタルなエコシステムにおける株式のようなものといわれることもあるが、仮想通貨はあくまで仮想通貨であって、収益分配を行う仮想通貨も一部存在するものの、株式のように経営に参画したり経営責任を追及したりする権利があるわけではない。

[50] 米国の民間ベースの分析では、他の金融資産などの価格との相関関係は小さいようである。http://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf

これはひとえに仮想通貨が将来生み出す有形・無形の価値の評価や期待の違いがもたらしているといえる。

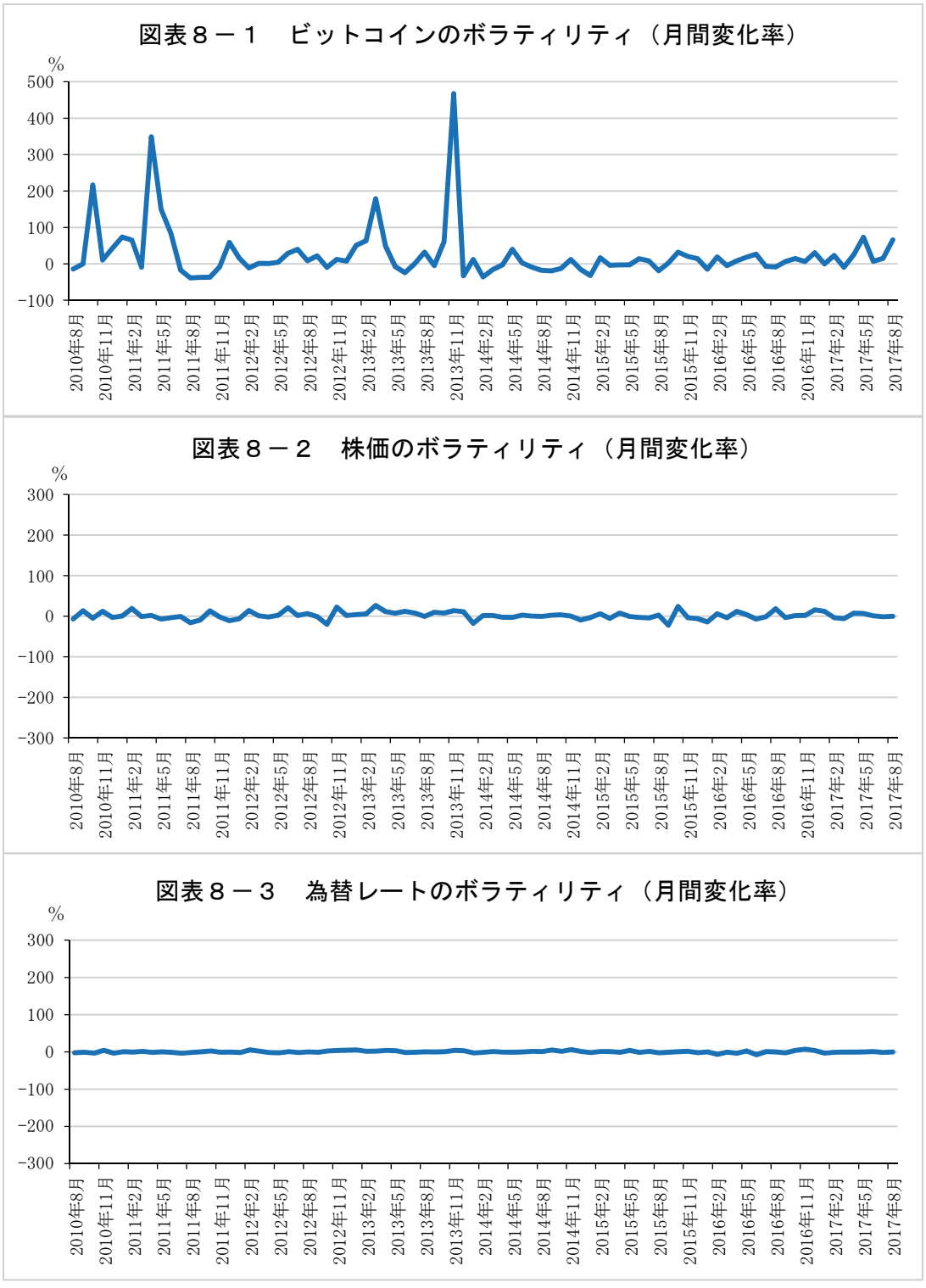
以上まとめれば、ビットコインなどの仮想通貨の価値は、ネットワーク（ブロックチェーン）に対する信頼、減価しにくい性格、送金コスト・手数料の安さや両替不要などの利便性、ブロックチェーンが生み出す社会的便益や期待などによると考えられ、その価格に対しては、供給が制限されていることから、これらの価値の評価が反映された需要が大きな影響を与えると思われる。現在は投資需要が大きいため価格変動が大きく、短期的には投機的動機がバブル的な状況を生み出すこともあると考えられる。

なお、ビットコインはしばしば金（ゴールド）と比較され、サイバー空間における金のような存在といわれることがある。この背景には金の不滅・不変性、稀少性がビットコインにも共通しているという発想があると思われ、実際、マイニングという言葉遣いにも鉱物資源を想起させるものがある。ただし、今日の通貨体制は金本位制ではなく、一般的受容性のある法定通貨を本位とし為替レートが決定されるシステムであり、上述のようなビットコイン（ブロックチェーン）の特徴が持続的な一般的受容性を生み、かつボラティリティの問題もクリアされれば、「通貨」として信任を得る可能性があるが、そうならなければ一つのデジタルな資産にとどまることとなる。

（３）仮想通貨のボラティリティ

仮想通貨は他の金融資産や法定通貨と比較してボラティリティが大きいといわれる（図表８）。しばしば価格が大きく低下し、その後さほど間をおかずに価格が低下前の水準まで戻るような動きを繰り返すこともあり、これは株式などでは余り見られない傾向である。仮想通貨はボラティリティが大きいがゆえに価値が安定せず、「通貨」として信認を得ることは難しいであろうとの指摘も多い。

仮想通貨がこのような動きをみせるのはなぜであろうか。過去をみると、ビットコインの価格が特に大きく変動しているのは、①不正使用が明るみに出たとき（６．参照）や取引所が破綻したとき（マウント・ゴックス事件）、②中国などで政策の転換があったとき（５．（２）①参照）、さらに③2017 年春以降の需要増大期やハードフォーク（ビットコイン・キャッシュの誕生）があったときなどである。これは、市場がまだ未成熟で資金量も小さく投資家が「情報に踊らされやすい」ことが背景にあるようにも思われ、市場規模が拡大して取引の



（注１）月間変化率（%）は、｛（月末価格－前月末価格）／前月末価格｝×100 で計算。
（注２）株価は、時価総額や成長性がビットコインと類似しているソフトバンクを用いた。
（注３）為替レートは東京市場ドル・円スポット相場。
（注４）ビットコインの 2014 年以降のボラティリティは、2013 年以前より相対的に小さくなっているが、株式・通貨より大きい。

（出所）筆者作成

厚みが増せば落ち着いてくるかもしれないが、実需と投資（投機）のバランスがとれないまま推移するなら変動が続く可能性もある。

ビットコインなどの仮想通貨に標準的な金融理論が適用できるかどうかは必ずしも明らかではないが、一般的には、金融資産のボラティリティが大きいということは成長のポテンシャルが大きいということでもある。ビットコインやイーサリアムなどの市場規模や価格がトレンドとして大きく拡大・上昇していることからみれば、ボラティリティが大きくなることはある意味、やむを得ないことなのかもしれない。また、一般に投資資産は同じリスクに対してリターンがどの程度になるかが重要であるが、この代表的な指標であるシャープレシオでみるとビットコインは他の金融資産などより優れているようである[51]。今後は、先物や証拠金取引（ＣＦＤ）、取引所間の裁定取引[52]、上場投資信託化（ＥＴＦ化）、オプション取引[53]などの環境整備により取引の厚みが増していけばボラティリティがより抑えられる可能性があるように思われるが、機関投資家・ファンドが投資対象に含める動きが本格化したり、アルゴリズム取引が行われるようになるなら変動が続く可能性もあることに留意が必要であろう。

もともと我が国では、ベンチャー投資などボラティリティが大きなファイナンスは欧米ほど活発ではないが、2017 年春以降は従来になく日本円の投資資金が仮想通貨市場に流入し、同年８月末現在のビットコインの取引通貨はドルを抑えて円の割合が最も高くなっている[54]。これは、必ずしも我が国にはリスク回避志向の投資家ばかりが存在するわけではないという見方ができる一方で、仮想通貨は新しい投資対象であり、リスクとリターンについての十分な理解がないままに投資が活発化している可能性も否定できない。ちなみに米国では、安

---

[51] 出典は脚注 50 に同じ。

[52] 仮想通貨の価格は、現時点では、流動性の問題などを背景に国による違いなどが恒常的に発生している。

[53] 米国証券委員会（ＳＥＣ）は 2017 年３月、ビットコインのＥＴＦの申請について、市場が規制されていないことから認めない判断を下したが（https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf）、同年７月、仮想通貨のオプション取引所などを運営するレッジャーＸ（Ledger X）は、初めて米国商品先物取引委員会（CFTC）から認定を受けた。したがって、現時点では判断は分かれているが、いずれＥＴＦも認められる可能性はあるように思われる。ちなみに米国ではビットコイン価格に連動するプロ投資家向けの投資信託は既に存在している（http://www.otcmarkets.com/stock/GBTC/quote）。

[54] https://www.cryptocompare.com/coins/btc/analysis/JPY。外国為替証拠金取引（ＦＸ）を含んでいる。

定的な資金運用の重要性が高い年金基金もハイリスク・ハイリターン投資の典型であるＶＣ（ベンチャーキャピタル）に投資している。投資割合は数％程度までのようであるが、リスクをとることでリターンがもたらされるという基本を踏まえ、ポートフォリオ全体でバランスをとることで実現している。年金基金のＶＣへの資金供与は我が国でもわずかに存在するようではあるが、いずれにせよバランスのとれた投資の重要性は仮想通貨投資を行う場合であっても例外ではない。

５．ＩＣＯと仮想通貨の普及・影響

（１）ＩＣＯの現状と課題

仮想通貨はＩＣＯ（Initial Coin Offering：新規通貨公開）を行うことで不特定多数の人々が投資できるようになる。これは株式におけるＩＰＯ（Initial Public Offering：新規株式公開）に相当するものであるが、株式とは異なりネット上で行われ、クラウドファンディングの形で資金が調達される[55]。ＩＰＯが企業の立ち上げ・経営に必要な資金調達のために行われるのと同様、ＩＣＯもネット上で仮想通貨を利用するプロジェクトを立ち上げ運営するための資金調達を目的として行われ、スケジュールなどはウェブサイトに掲載されている[56]。

2017 年に行われたＩＣＯは８月末現在で 125 件、総資金調達額は 1,600 億円に達しており[57]、特に資金調達額の大きなＩＣＯは図表９の通りであるが、ＩＰＯを行った企業が必ずしも順調に成長するわけではないのと同様、ＩＣＯを行った仮想通貨も目的・用途が明確でなかったり、ビットコインやイーサリアムと比較すれば小粒で骨太さに欠けるなど、将来性に疑問符がつかざるを得ないケースが多いとされる[58]。ＩＰＯにおいて定められている会計監査や上場審査のようなルールがＩＣＯには存在しないことと相俟って、現時点ではＩＰＯに対する投資よりはるかにリスクが大きいようである。

---

[55] クラウドセール、トークンセールなどともいわれ、一般にビットコインやイーサリアムなどの仮想通貨で払い込まれる。ＩＣＯの前にプレセールが行われることもある。

[56] https://www.coinschedule.com/など。

[57] https://www.coinschedule.com/stats.php

[58] 近時のＩＣＯはビットコインのように通貨そのものとしての利用を目指すものもあるが、様々な Dapps（分散型アプリケーション）のプラットフォームとしての機能の提供を標榜するものも多い。その際、プラットフォームとして独自通貨ではなくイーサリアムを利用するものも相当数存在するが、収益分配型のトークンについては今後、関連法令に準拠する形になるであろう。また、近時のＩＣＯはＤＡＯ（自律分散型組織）を標榜するものも多いが、理念が先行しており内実が伴っていないとの批判がある。

図表９　今年の資金調達額が大きなＩＣＯ案件（2017 年８月末現在）

１　Tezos（トークン：XTZ）250 億円
ビットコインやイーサリアムのような独自の仮想通貨を目指す。コンセンサスアルゴリズムＰｏＳ。トークン保有者の投票によりハードフォークによらないルールの修正を実現するとされる。

２　Bancor（トークン：BNT）160 億円
独自の価格発見機能を用いて、仮想通貨や地域通貨の価格付けを行い交換可能とする。分散型の通貨取引所のような機能を担うことが可能とされる。

３　Status（トークン：SNT）100 億円
イーサリアムのモバイル化。イーサリアムのネットワークにモバイルからアクセスし、Dapps などのプラットフォームとなることを実現するとされる。トークンはイーサリアムにペッグ。

４　TenX（トークン：PAY）70 億円
非プリペイド型（チャージ不要）の仮想通貨デビットカード。日本円対応。カード利用者へインセンティブとして PAY やイーサリアムを還元するとされる。

５　MobileGO（トークン：MGO）50 億円
グーグル、アップルの寡占状態となっているモバイルゲーム市場において新たなプラットフォームを構築するとされる。ゲーム開発者の支払額をグーグル、アップルより低率に設定。

（注）資金調達額が大きいことは必ずしも成功を意味しない（TheDAO の例あり）

（出所）ウェブサイト情報などに基づき作成

ただし、ビットコインやイーサリアムも当初から評価されていたわけではないし、今後、これらを凌駕する仮想通貨が現れないとも限らない。ＩＰＯにより生まれるベンチャー企業が経営不振に陥ってもＩＰＯという制度自体に罪はないのと同様、仮想通貨が多産多死であってもＩＣＯという制度自体を否定することは適切でない。リスクを逆手にとって考えれば、ＩＣＯは基礎研究やシーズ発掘などの見返りが期待できない（しかし多大な利益をもたらす可能性もゼロではない）資金提供となじむ可能性もあるし、近時では、国家がＩＣＯを利用して資金を取り込もうとする構想も表明されている[59]。

ＩＣＯは今後押し寄せてくるであろう、情報と金融が合体した情報資本主義

[59] 従来から電子政府化を推進しているエストニアでは、ボーダーレスなデジタル国家の実現を目指して、イーサリアムの開発者 Buterin 氏の支持のもと、ＩＣＯにより「エストコイン」（Estcoin）と呼ばれるトークンを発行することが検討されている。そこには、海外の人々にエストニアの「e-レジデント」となって資金拠出してもらい、国家建設を進めようという意図もあるとされる。ただし、エストニアの法定通貨はユーロであることから、エストコインは一種の政府通貨（あるいは国債類似のもの）を意図しているようにも思われる。

の第一波のような印象もあり、資本主義の初期的形態に似た荒々しさがある。ＩＣＯへの投資を行うとするなら、ネット上で公開されているホワイトペーパーや開発者・コミュニティのバックグラウンドなどを含め納得できるまで情報収集を行い、リスクの大きさを十分認識することが最低限必要である[60]。

（２）内外での普及の現状と可能性

①普及の現状

現在、仮想通貨の利用者は世界でどの程度存在するのであろうか。よく知られたインターネット上のウォレット（口座）の１つである「Blockchain.info」の統計によれば、同ウォレットのユーザー数は 1,600 万強となっているが[61]、開設自体は簡単にできることから、アクティブに使われていないケースもあると思われる。一方、ケンブリッジ大学の 2017 年の推計[62]によれば、現在アクティブな仮想通貨のウォレット数は 580 万～1,150 万の間であり[63]、一人の利用者が平均して二つのウォレットを保有しているとの仮定のもと、290 万～580 万人がアクティブに仮想通貨を利用しているとされている。この数字は 2015 年には 70 万～290 万人であったので、1 年で 100 万人以上のペースで増加しており、そう遠くない将来、アクティブな利用者数が 1,000 万人を超える可能性は高いと思われるが、それでも世界の人口に占める割合は 0.2%に満たない。なお、世界の仮想通貨取引所に開設されている口座数については定かではないが、桁数としては上述のウォレット数と同じ位ではないかと推測される。

ビットコインに対応可能な店舗数は、報道によれば 2016 年に世界全体で 10 万店を超える程度のようである。我が国でも使用可能な店舗は増加しており、

---

[60] 実際には情報が限られているケースが多いと思われ、第３者関与のルールの設定などでＩＣＯの質を担保することが望まれる。これは経済学でいうところの「逆選択」（ＩＣＯの質が全般的に低下してしまう状況）を防止するためにも役立つと考えられる。なお、株式とは異なり仮想通貨には経営に参画する権利がないことから、投資後の「モラルハザード」（ＩＣＯ実施者の懈怠行為など）も生じやすいと考えられる。

[61] https://blockchain.info/ja/charts/my-wallet-n-users

[62] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[63] 自らが保有・管理する口座数であり、仮想通貨取引所に開設されているアカウント数や仮想通貨の決済サービスにおける保管数は含まれないため、保守的な数字である。活用されず長期保管のみ行っているような口座を含めればこの何倍かになるとされる。なお、マネックス証券の 2017 年６月の調査(https://info.monex.co.jp/survey/pdf/survey_201706.pdf)によれば、個人投資家のうち仮想通貨への投資を既に実行している割合は日米で３％、香港で 10%程度である。

同年に数千店であったが、現在では店舗におけるビットコインのモバイル決済も可能となりつつあることから、さらなる増加が予想される。

ビットコインは我が国よりも海外の方が早くから普及している[64]。2013 年のキプロスの金融危機や 2015 年のギリシャの経済危機の際には、銀行が営業停止になったり預金の引き出しが制限されたりしたが、ビットコインのＡＴＭで現金化が可能であり、ビットコインの保有者は相対的に影響が軽減されたようである。ちなみに現在、キプロスのニコシア大学(The University of Nicosia)はビットコインで学費を支払うことが可能であり、デジタル通貨の修士課程がおかれている。2015 年にウクライナでハイパーインフレが発生し通貨フリヴニャ（グリブナ）が急落した際にも、ビットコインへの需要が高まったといわれる。最近では、持続的なインフレと政情不安に悩まされているベネズエラでビットコインの需要が増大しているようである。

ウェブサイト情報[65]によれば、2017 年８月末現在、欧州諸国（ウクライナ、スペイン、ポーランド、ブルガリア、ルーマニア、スイスなど）や米国、カナダ、オーストラリアなどでは、ビットコインなど仮想通貨のＡＴＭや仮想通貨と法定通貨の交換場所（銀行の兼用ＡＴＭ、小売チェーンやキャッシャー・デスクなど）が少なくとも 1,000 か所以上、多い国では１万か所以上存在している（我が国は 17 か所)。この他、比較的ビットコインの認知度が高いと思われるのは英国[66]、オランダ、チェコ、台湾、韓国、アルゼンチンなどである。

なお、中国、ロシア、インドは３国で世界の人口の４割近くを占め、ある意味、仮想通貨の将来の鍵を握る国々である。報道によれば各国とも仮想通貨の性格に対して警戒感を抱きつつ規制の在り方を検討しているようであり、特に中国ではこれまでも規制と緩和（容認）が繰り返されてきているが、2017 年９月には規制強化策（国内取引所の閉鎖）が報道された。資金の国外流出への懸念などが背景にあるとされるが、ＩＣＯの禁止と同様、永続的なものかどうか

---

[64] 一般にビットコインの普及は、各国・地域で草の根的に受容されて法定通貨と交換可能となることで進んできているが、政府（中央銀行）の受け止め・対応は、法定通貨への影響や資金流出への懸念（国家の威信)、マネーロンダリングやテロ、犯罪対策などの観点から批判的な場合もあれば、フィンテックや金融産業・イノベーション振興、ひいては経済発展への貢献などを重視して容認姿勢の場合もある。中国は振れが大きいが、(成功するかどうかは別として）自国経済に不安定化をもたらさないような、また成長を阻害しないようなコントロールを意図しているという意味では一貫しているのかもしれない。

[65] https://coinatmradar.com/

[66] 2016 年のブレグジット決定時に需要が増大したといわれる。

現時点では必ずしも自明ではない[67]。一方、ロシアはブロックチェーンやデジタル経済化への関心が強いといわれること[68]、インドも高額紙幣を廃止しデジタル経済化へと舵を切り、仮想通貨への関心も高まっているといわれることなどから、短期的には規制強化もあり得るものの中長期的な方向性としては容認される（禁止しても実効が上がらない）のではないかと推測される[69]。

②海外での普及の可能性

ビットコインなどの仮想通貨は、銀行口座を保有していない低所得層の金融アクセス改善に貢献する潜在性を有している。世界銀行の 2015 年の報告書[70]によれば、ネットを含め銀行口座を保有していない成人の数は、減少傾向とはいえ世界中で約 20 億人存在し、中でも途上国の下位 40%の低所得世帯では半数以上が銀行口座を保有していない。他方、サブサハラ・アフリカ地域では成人のモバイル口座保有者が増加しており、世界全体ではわずか２％であるモバイル口座保有率は、同地域では 12%に達している。特にケニアでは成人の 58%がモバイル口座を保有しており[71]、成人の半数以上が光熱費の支払に携帯電話を利用している。さらに、コートジボワール、ソマリア、タンザニア、ウガンダ、ジンバブエでは、モバイル口座を保有する人口が金融機関の口座を保有する人口を上回っている。

一般にデジタル化・モバイル化は、現地通貨（法定通貨）が対象となることはもちろんであるが、ブロックチェーンに基づくビットコインなど仮想通貨もトレーサビリティが高く、諸外国からの寄付[72]を含む支援と連動させることも容易であり、身分証明（ＩＤ）などの機能を持たせることも可能と考えられ

---

[67] 中国国内の取引所が閉鎖されれば短期的には混乱は避けられないであろうが、Ｐ２Ｐネットワークを含め世界に広がるビットコインのエコシステムがなくなることは考えられない。現時点ではマイニングプールをはじめ仮想通貨界における中国のプレゼンスは多大であるが、政策の振れも大きいことから、中長期的にプレゼンスが一定程度にとどまるなら、むしろ仮想通貨市場の安定につながる可能性もあるかもしれない。

[68] イーサリアムの開発者 Buterin 氏はプーチン大統領と面会している。大統領はロシア生まれでロシア語が堪能な Buterin 氏の存在もあり、仮想通貨に関心を有しているとされる。

[69] ただし、中国やロシアは法定通貨のデジタル化を検討しており、ビットコインなど「民間版」仮想通貨より「国家版」仮想通貨を重視する可能性もあるように思われる。

[70] http://www.worldbank.org/ja/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report

[71] エムペサ（M-PESA）といわれるショートメッセージ（ＳＭＳ）を利用したモバイル送金サービスが普及している。

[72] 寄付を匿名で行いたい場合には仮想通貨（ビットコイン）は役に立つであろう。

る[73]。いずれにせよ低所得層のスマホ普及率を高め、ユーザーの選択肢を広げることは、送金コストの低下など世銀が掲げる持続可能な開発目標の実現のためにも有用であり、衛星通信によるインターネット環境の整備などを含め、地球上のあらゆる地域で選択肢に含められるよう対応を進めるべきであろう。

（３）経済への影響

仮想通貨は現在、経済的にどの程度の重みを持つのであろうか。我が国の金融資産や通貨の残高（ストック）を大雑把にみると、個人金融資産 1,800 兆円、株式時価総額 600 兆円、通貨（紙幣・貨幣）流通高 100 兆円、マネーサプライ（マネーストック、Ｍ３）1,300 兆円程度である。世界全体でみれば、個人金融資産や株式時価総額は我が国の 10 倍超、通貨流通高やマネーサプライは５倍超になるであろう。これに対して 2017 年８月末現在の仮想通貨の市場規模は 17 兆円程度であるから、割合比が最も高くなる通貨でみても仮想通貨は３％強を占めるに過ぎず、ビットコインだけなら２％弱である。

したがって、仮想通貨は現在、資産市場においてマイナーな存在でしかないが、将来的に市場規模が現在より一桁位拡大するような状況が出現するなら、金融市場、ひいては一国の経済に何某か影響を与えるであろう。その方向性としては、ブロックチェーンの普及が様々な分野で大きな需要をつくり出すことで好影響がもたらされる可能性が高いのではないかと思われるが、一方で仮想通貨の供給量が制限されていることが悪影響を及ぼすという指摘もある。例えば、イングランド銀行の 2014 年の報告[74]では、仮想通貨の供給量が制限されていることが経済にデフレをもたらし、消費の先送り・需要低下と供給の減少が生ずる一方で失業率は増大するとされており、ＩＭＦの 2016 年のペーパー[75]でも、仮想通貨にはデフレリスク、金融ショックや景気変動への対応が非弾力的になるリスク、最後の貸し手としての役割を果たせないリスクがあるとされている。

---

[73] 既にウェブサイト上で、2015 年に欧州で発生した難民問題への対応として、ブロックチェーン上での難民の身分証明（ＩＤ）や、ビットコインの寄付を原資とする難民へのデビットカードの交付などを行うプラットフォームが立ち上がっている（https://bitnation.co/refugee-emergency-response/）。ちなみに仮想通貨対応のデビットカードは海外を中心に複数存在している。

[74] http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

[75] https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

中央銀行やＩＭＦなど通貨当局のこのような見方は、仮想通貨（ビットコイン）を生んだサトシ・ナカモトの思想とは一見、異なっているようにみえるが、この違いは、実は同じコインを表からみるか裏からみるかの違いに過ぎないようにも感ぜられる。すなわち、通貨当局からみれば、ビットコインは金融危機が生じたときに流動性供給の役割を担うことができず、不安定化をもたらす悪しき通貨なのであろうが、ビットコインサイドからみれば、ビットコインは過剰流動性がもたらしたリーマンショックへの反省から生まれ出たものであり、金融バブルが生ずることのないように供給量に縛りをかけたのだということになる。もちろん最終的に金融・通貨システムの安定化に責任を負うのは通貨当局であり、今後も万が一危機的な状況が生じれば適時適切に対応措置がとられなければならず、この役割はビットコインには果たせない。ビットコインはあくまでもボーダーレスで自律的、分散的な存在であり、国家・地域の経済情勢などの影響を受けて需要が変動することはあっても、法定通貨を代替するような性格のものではないといえる。

６．仮想通貨の注意点

仮想通貨は口座名に実名が使われず匿名性があることから、マネーロンダリングやテロ、犯罪などとの結びつきを懸念する声も多く聞かれる。2013 年には、米国の違法薬物や銃器などを扱う闇サイト「シルクロード」がＦＢＩに摘発され、取引に使われていたビットコインが没収された。当時のビットコインの大きな価格変動はこの事件と関係があると思われる。ただしビットコインは、匿名ではあるが取引が全てブロックチェーン上に記録されオープンになることから、資金の流れはむしろ追跡しやすいとの指摘や、匿名性という点では紙幣など現金も同様であるとの指摘もある。我が国では 2017 年４月以降、取引所において口座開設者の身元確認が行われるようになっており、このような確認や取引所の免許制・登録制が世界の隅々まで浸透していくことが望まれる。

仮想通貨についてはサイバー攻撃のリスクもしばしば指摘されており、近時も、北朝鮮のハッカーが韓国の仮想通貨取引所への攻撃を強めていると報じられた。免許制・登録制の取引所はセキュリティ対策の水準が向上しており、二段階認証（ＩＤ・パスワード認証＋ワンタイムパスワード等認証）や暗証番号の設定を前提に、ネットバンキングなどと比較して特にリスクが高いわけではないとの見方がある一方で、ハッキングの恐れは常に存在し秘密鍵が盗まれる恐れもあることから、特に長期保管するような場合には取引所におかず、インターネット環境から切り離された個人用のハードウェア・ウォレットを使うべ

きであるとの主張もある。しかし後者の場合でも誤操作や誤作動、紛失・盗難の可能性などは排除できないことから[76]、どのような方法でも100%安全ということはないのであり、取り扱う場合には常日頃から安全な保管の在り方に対する意識を高めておく必要がある。

仮想通貨を巡っては企業会計や税制上の論点も指摘されている。企業や個人が仮想通貨の取得・譲渡・出資、仮想通貨と法定通貨、仮想通貨間の取引（国境をまたぐ取引を含む)、ＩＣＯなどを行った場合の会計上、税制上の扱いについては必ずしも明確でないところがあるといわれる。仮想通貨には通貨としての側面と価値が増大（変動）する資産としての側面があることから、外国為替証拠金取引（ＦＸ）や他の金融資産に対する課税（税率、損益通算）とのバランスなども課題となり得るであろう。いずれにせよ企業会計や金融課税全体の中での仮想通貨の位置付け・評価の確立・定着には一定の時間がかかるのではないかと思われる。

仮想通貨についてはいわゆる詐欺コインの問題もある。仮想通貨と称しつつ、一般的なウェブサイト（https://coinmarketcap.com/など）に掲載されておらず、ＩＣＯも行われていない正体不明のコインの勧誘が行われており、ネズミ講のような仕組みの詐欺コインも存在しているようである。５.（１）でも指摘したが、仮想通貨はあくまでもインターネット上の存在であり、投資を行うなら必ず仮想通貨・ＩＣＯの一覧が掲載されたウェブサイトなどを複数閲覧し、内容を確認する必要がある。

７．おわりに－銀行の取組と通貨の将来

通貨のデジタル化、インターネット化の流れは、トークンとしての通貨発行の容易化をもたらし、極論すれば誰でも「通貨らしきもの」を発行することができるようになった（トークンエコノミー)。現行法令との整合性に留意する必要はあるが、仮想通貨にはビジネスから学術、ゲーム・趣味に至るまで様々な領域にチャンスや面白さをもたらす潜在力がある。もちろん通貨としてみればドルや円、ユーロなどの法定通貨に比較優位性（一般的受容性）があることはいうまでもなく、直ちに情勢が変化するとも思われないが、これまで通貨とい

[76] ウォレットなど仮想通貨関連ハードウェアの国産品はほとんど存在せず、マニュアルが外国語の場合もある。ユーザーフレンドリーな保管環境とセキュリティ確保の両立を高いレベルで実現することは今後の課題の１つと考えられ、商品・サービスの開発を含めた対応が期待される。

えば法定通貨を意味していた世界に新たな考慮要因がもたらされたことは間違いない（図表 10)。

図表 10　仮想通貨の見通し（まとめ）

ビットコインに代表される仮想通貨は、

→ボーダーレスな存在、画期的イノベーション（ブロックチェーン）の具現化であり、日々変化しているため将来を見通すことに難あり。一方、中国、ロシアなどの法定通貨のデジタル化が国際通貨システムのバランスを変化させる可能性あり

→批判されてもなくならないのはユーザーが価値を感じているから（感じなければ消失）

→ドルのような基軸通貨圏（国家）より、高インフレなど法定通貨が問題を抱える国・地域の方が切実なニーズあり。我が国もビットコイン対応可能店舗は増大

→銀行口座を持てない低所得者（アフリカに多い)、本国への送金が必要な移民などにおいて潜在的なニーズ大

→マイニングの過半を行う中国が影響力を有し、ロシアも関心を高めている状況。仮想通貨をみる目は、自国の繁栄（経済成長）に役立ち利益を害さないかどうか

→発行限度があり緩和的な金融政策は担えず、法定通貨を代替するものとはならず

→成長の潜在性を有し、法定通貨との全体最適を考える必要。金融政策に支障が生じないよう、必要に応じた規制も正当化

→（制度論は別として）民間銀行の発行可能性は必ずしも明らかではないが、現実問題としてビットコインと互していくためには相当な努力が必要（成功は僅少？）

→中央銀行も発行する可能性があり、いずれスウェーデンや中国、ロシアなどからデジタルな法定通貨が導入されるであろうが、ボーダーレスで管理になじまないビットコイン型ではないと予想。モバイル通貨が普及すれば預金通貨の不要論も生じ得るが、現時点では不確定性あり

（出所）筆者作成

報道によれば、三菱 UFJ フィナンシャルグループはブロックチェーン上で「MUFG コイン」を発行し、利用者同士がコインをやりとりしたり、店舗での支払いなどに利用可能なものとする構想を進めているという。みずほフィナンシャルグループとゆうちょ銀行、一部の地銀も同種の「Ｊコイン」を発行する構想があると報道されている。これらのコインは円にペッグするとされ、独自の価値を追求するものではないことから、自律的、分権的なシステムへの信頼などから価値(一般的受容性)が生み出されるビットコインとは異なっており、送金機能がついた電子マネーのようなものにも思われる。ちなみに、円やドルなどの法定通貨にペッグしている場合には仮想通貨法上の仮想通貨には該当しないので、報道されているコインを仮想通貨と称することには筆者は抵抗がある。

諸外国の大手銀行がこのような「通貨」にどの程度関心を有するかは必ずしも明らかではないが[77]、勝ち残れるかどうかはユーザーがメリットを感ずるかどうかによるであろう。民間銀行が仮想通貨を発行することは現時点では制度的に難しいであろうが、銀行が「通貨」を発行するというのであれば本来、想定されるのはやはり既存システムの延長線上ではなく新たなブロックチェーン上で、自らの信用を背景に一般的受容性に基づいて価格が形成されるようなトークン、すなわち仮想通貨ではないか[78]。このような仮想通貨であればボーダーレス性も必然的に備えることとなるが、それにしても国際送金の手数料などでビットコインと互していくためには相当な努力が必要で、成功は容易ではないであろう。

デジタル通貨の発行は中央銀行も関心を有している。通貨のスマホ化が進展する中で、中央銀行もブロックチェーン上で通貨を発行するようになれば、個人同士（Ｐ２Ｐ）はもちろん、中央銀行が個人の同行口座（モバイル口座）と直接やりとりを行うことも容易になり、預金通貨を含む金融・通貨システムに大きなインパクトをもたらす可能性がある[79]。民間銀行も「通貨」を発行するというならそれは本来、このような通貨の将来やビットコインなど仮想通貨への対応を視野に入れたプロポーザルなのではないかと筆者は邪推しているが、第一歩を踏み出した後、どのように発展していくこととなるのか注目される。

法定通貨のデジタル化については、諸外国でも一般国民を対象とするデジタル通貨の発行が具体的に検討されるには至っていないようであるが、日銀のレ

---

[77] シティバンクやニューヨーク・メロンバンクなど一部行が独自通貨を実験的に発行しているが、その性格（仮想通貨といえるものであるかどうかなど）は必ずしも明らかではない。海外の大手銀行もおしなべてブロックチェーンに対する関心は高いものの、ビットコインのような仮想通貨や独自通貨に対する受け止め（評価・距離感）は様々のようである。ＪＰモルガン・チェースのジェイミー・ダイモンＣＥＯはビットコインの痛烈な批判者として知られるが、何が批判の矛先なのか、ドルへの影響や自社・顧客利益への懸念なのか、あるいは発行の限定なのか（モルガン財閥の創始者Ｊ・Ｐ・モルガンは連邦準備制度がなかった 1907 年恐慌時に自己資金を提供して深刻化を食い止めたことで知られる）、筆者は判断材料を持ち合わせていない。

[78] MUFG コインやＪコインが分権的ではないように思われる点もビットコインとは異なっているが、既述のようにブロックチェーンの設計において、一定の管理の余地を残してトークンを成立させることは可能と考えられる。

[79] 一般にこのような「強力」なデジタル通貨が発行される可能性については、中央銀行の独立性なども踏まえつつ慎重に検討されるのではないかと思われるが、仮に発行される場合でも、いわゆる政府通貨（政府紙幣）とは峻別されなければならないであろう。

ビュー[80]などによれば、オランダ、カナダなどの中央銀行では実証実験が行われ、イングランド銀行は既述の報告を公表して検討を続けている。シンガポールの中央銀行でも法定通貨をブロックチェーン上でトークン化する可能性について検討され、中国やスウェーデン[81]の中央銀行はいずれ先行してデジタル通貨を発行する可能性があり、ロシアもプーチン大統領の関心が高いといわれる。そして日銀も欧州中央銀行（ＥＣＢ）と共同で決済システムへのブロックチェーンの適用に関する実証実験を行っている[82]。

デジタル通貨はマイナス金利の容易化など金融政策の自由度・即効性を高め、中央銀行にとって望ましいものであるとの見方もあるが、我が国では現金志向が強いことから、高額紙幣を含め現金をなくすことは容易ではないと思われ、相当な期間、共存を図らなければならないであろう。その場合、デジタル通貨と現金の金利に差異が生じたり、交換比率が変動したりすることも生じ得るように思われるが、デジタル通貨が相対的に選好されない懸念があるとすれば、何某か人為的に対応しなければ普及していかないかもしれない。いずれにせよ中央銀行も、通貨以外に資産・負債の管理などを含めデジタル化していくことは世界的な流れではあろうが、金融政策の企画立案・実施などデジタル化が困難な部分にも本質的な価値があり評価を受ける可能性が高いことはいうまでもない。

もともとリバタリアン的思想になじみ管理を嫌うビットコインなど仮想通貨に対する中央銀行の風当たりは強く、いずれ責任を有する立場から排斥するようになるという論調もみられるが、仮想通貨はあくまでボーダーレスな存在で「異次元の住人」ともいえることから、法定通貨がデジタル化したとしても必ずしもライバルになるとは限らない。各国の財政金融政策が法定通貨により行われるのは極めて自然であり、仮に中央銀行がブロックチェーン上でデジタルな通貨（すなわち仮想通貨）を発行することとなっても、裁量よりルールを重視し発行上限があるビットコイン型にはならないであろう。

仮想通貨の市場規模が現在より一桁位拡大すれば金融政策に何某かの影響を与えるであろうが、それにしても資産としての仮想通貨と、通貨としての仮想通貨がバランスしながら成長するとは限らず、少なくとも筆者にはデジタル化

[80] https://www.boj.or.jp/research/wps_rev/rev_2016/data/rev16j19.pdf
[81] スウェーデンはキャッシュレス化への先進的取組で知られており、デジタル通貨流通の土壌が整いつつある。
[82] http://www.boj.or.jp/announcements/release_2017/data/rel170906a3.pdf

した円やドルがビットコインやイーサリアムに脅かされる姿は想像できない。むしろ仮想通貨の成長はこれまで以上に法定通貨の本質を際立たせ、必要に応じた規制の正当化をもたらす可能性さえある（もちろん好都合なことばかりではないであろうが)。

ただ、やはり仮想通貨は若い通貨で爆発力があり、力で抑え込もうとしても空回りしたり、一般的受容性の獲得を巡って法定通貨と事実上競合する場合もあり得ること、今後、デジタルな法定通貨が内外でどのように普及していくかが現在の国際通貨システムのバランスに変化をもたらす可能性も否定できないことなどから、金融・通貨当局において、どのようにすればユーザー（国民）の満足度が高まり全体最適が達成されるか、そして国富の増大がもたらされるかという観点から必要な育成や介入を行い、国際的に協調しつつ総合的に通貨環境の整備を図っていく方法論が求められるように思われる。

【参考文献】

岩村充『中央銀行が終わる日』新潮選書、2016 年

館龍一郎・浜田宏一『金融』(現代経済学６)、岩波書店、1972 年

野口悠紀雄『ブロックチェーン革命』日本経済新聞出版社、2017 年

マイケル・Ｅ・ポーター「共通価値の戦略」(『ハーバード・ビジネス・レビュー』2011 年６月号、ダイヤモンド社)

Andreas M. Antonopoulos, *“Mastering Bitcoin”*（アンドレアス・Ｍ・アントノプロス『ビットコインとブロックチェーン』今井崇也・鳩貝淳一郎訳、ＮＴＴ出版、2016 年）

Ronald H. Coase, *“The Firm, The Market, and The Law”*（ロナルド・Ｈ・コース『企業・市場・法』宮沢健一・後藤晃・藤垣芳文訳、東洋経済新報社、1992 年）

Arvind Narayanan, Joseph Bonneau, Edward W. Felten, Andrew Miller and Steven Goldfeder, *“Bitcoin and Cryptocurrency Technologies”*（アーヴィンド・ナラヤナン／ジョセフ・ボノー／エドワード・Ｗ・フェルテン／アンドリュー・ミラー／スティーヴン・ゴールドフェダー『仮想通貨の教科書』長尾高広訳、日経ＢＰ社、2016 年）

Nathaniel Popper, *“Digital Gold”*（ナサニエル・ポッパー『デジタル・ゴールド』土方奈美訳、日本経済新聞出版社、2016 年）

Kenneth S. Rogoff, *“The Curse of Cash”*（ケネス・Ｓ・ロゴフ『現金の呪い』

村井章子訳、日経BP社、2017年）
Don Tapscott and Alex Tapscott, *"Blockchain Revolution"*（ドン・タプスコット／アレックス・タプスコット『ブロックチェーン・レボリューション』高橋璃子訳、ダイヤモンド社、2016年）
Andreas M. Antonopoulos, *"The Internet of Money"*, Merkle Bloom LLC, 2016
Richard Ozer, *"Ethereum"*, CreateSpace Independent Publishing Platform, 2017
Paul Vigna and Michael J. Casey, *"The Age of Cryptocurrency"*（2016 edition）, Picador, 2016

（内線75180）

［補遺１］リップル（トークン：XRP、市場規模１兆円（2017年８月末現在））

・リップル（Ripple）は2004年頃から検討が進められ、2012年に正式に立ち上げられた。仮想通貨というよりも金融機関を対象としたデジタルな送金ネットワークのインフラ、あるいはプロトコルとしての性格を有するものであり、株式会社であるリップル社が管理するネットワークであるところに特徴がある。他の仮想通貨と同様に分散型の台帳が用いられてはいるが、ＰｏW、ＰｏＳ型のコンセンサスアルゴリズムではなく、同社主導のコンセンサス・システムに基づく方式となっており、ビットコインやイーサリアムと同様のブロックチェーンは用いられていない。他方で承認には時間を要さず、数秒程度で送金が可能とされる。

・送金時に手数料として費消されるトークンがリップル（XRP）であり、リップル社が法定通貨や他の仮想通貨との交換を保証する。発行枚数は1,000億XRPで全て発行済みであり、過半をリップル社が保有しているようである。異なる通貨同士のやりとりなどもトークンとしてのリップル（XRP）が介在することで円滑に取引を成立させることができ、この意味でリップルは「ブリッジ通貨」としての役割を果たすものとされる。

・世界的なネットワークが確立されれば、従来の国際送金のように複数の銀行が介在しなくなるので、送金コストは下がるというのがリップル社の主張である。ただし、リップル（XRP）の価値を巡っては、①リップル自体が自律的・分権的なネットワークとしての価値を有しているわけではない、②トークンの機能が送金手数料やブリッジ通貨に限定されている（費消された分だけXRPが減少していく）、③リップル社から様々なステークホールダーへのダイレクトな供与について情報公開されていないなどの指摘もある。

・リップルは、ビットコインやイーサリアムのような理念主導のパブリックな存在というよりは現実的、企業コンソーシアム的な存在であり、実際に銀行などとの連携を深めている。我が国を含む世界の大手銀行などはGPSG(Global Payments Steering Group）というコンソーシアムを形成し、リップルを利用した国際送金に向けて標準ルールの策定などを行うとされている。

［補遺２］市場規模 10 位までの仮想通貨
（ビットコイン、イーサリアム、リップルを除く）

○ Bitcoin Cash（ビットコイン・キャッシュ、トークン：BCH）市場規模１兆円

2017 年～。ビットコインからハードフォークで分岐して成立。ブロックの容量が１MB から８MB に引き上げられているが、その他はビットコインと同様。

○ Litecoin（ライトコイン、トークン：LTC）市場規模 4,000 億円

2011 年～。ビットコインと同様の機能を持つ仮想通貨。ビットコインを「金」とすればライトコインは「銀」といわれる。コンセンサスアルゴリズムＰｏW。マイニングは一般的な CPU でも可能とされ、ブロック生成時間 2.5 分。発行上限 8,400 万 LTC。

○ ＮＥＭ（ネム、トークン：XEM）市場規模 3,000 億円

2015年～。ビットコイン2.0プロジェクトの１つ。コンセンサスアルゴリズムがＰｏＩ(Proof of Importance、残高・取引回数・取引量などから総合的にスコアリング）である点が特徴。NEM の技術は我が国の金融機関・民間企業が実証に関与しているプライベートブロックチェーン Mijin で使用され、国内のユーザーが多いとされる。発行上限約 90 億 XEM（発行済）。

○ DASH（ダッシュ、トークン：DASH）市場規模 3,000 億円

2014 年～。Ｘコイン→ダークコイン→ダッシュと名称変更。匿名性の強化に特徴があり、アドレスを暗号化して追跡を不可能化。コンセンサスアルゴリズムＰｏW。マイニング報酬の 10％を DASH 基金が取得し、残りをマイナーとマスターノードが均等に分け合う。ブロック生成時間数秒。発行上限 2,200 万 DASH。

○ IOTA（アイオータ、トークン：MIOTA）市場規模 2,600 億円

2015 年～。ＩｏＴ導入のための仮想通貨を標榜。ブロックチェーンとは異なる技術(Tangle)を使用し、利用者がマイナーとなり取引承認（コンセンサスアルゴリズムＰｏW)。送金手数料無料。発行上限 2,700 万 MIOTA（発行済）。

○ Monero（モネロ、トークン：XMR）市場規模 2,200 億円

2014 年～。DASH と同様の匿名性の強化が特徴で、送金の追跡を不可能化。コンセンサスアルゴリズムＰｏW。マイニングは一般的なＣＰＵでも可能とされ、ブロック生成時間 1～2 分。発行上限 1,840 万 XMR。

○ ＮＥＯ（ネオ、トークン：NEO）市場規模 1,700 億円

2015 年～。中国発のアプリケーション・プラットフォーム。イーサリアムのようなスマートコントラクトの実行機能を持ち、ブロックチェーン上で様々な資産をデジタル化。イーサリアムと異なり多くのプログラム言語が使用可能。コンセンサスアルゴリズムＢＦＴ（選ばれたノードによる承認)。ブロック生成時間 15～20 秒。発行上限１億 NEO。

※2017 年８月末現在。ウェブサイト情報などに基づき作成しているが、事実関係が異なる場合があり得る。