特別解説

応般

仮想通貨の現状と未来

―ビットコイン分裂とICOの拡大を中心に

岩下直行（京都大学公共政策大学院）

ビットコインの分裂と仮想通貨の高騰

2008年，Satoshi Nakamotoという正体不明の人物によるペーパー[1]からビットコインは生まれた．インターネット上で利用可能な電子現金を作ろうという実証実験プロジェクトは，1994年のDavid Chaumによるecashを始めとして，数多く試行されてきた．その理論研究は1982年のCRYPTOに提出された論文[2]にまでさかのぼる．こうした技術蓄積を持つ情報技術研究の世界から見れば，ビットコインはごくありふれた実証実験の1つにすぎない．

ところが，2017年8月の段階で，ビットコインを中心とする仮想通貨の交換価値は15兆円を超えるまで高騰しており，ビットコインの分裂に至るまでの経緯は，まるで世界を揺るがす大事件のように報道された．これはいったいなぜなのだろう．そして，分裂騒動を経て，今後，ビットコインはどう変化し，社会はそれをどのように受け止めていくのだろうか．

本稿では，ビットコインを巡る社会的，経済的な背景を含めて技術の内容を分析することにより，こうした疑問に答えていこうと思う．

電子現金の系譜：ChaumとSatoshi

電子現金と呼ばれる技術の生みの親が，高名な暗号学者，David Chaumであることは，情報技術の世界では常識であろう．彼は1982年の論文で，将来，コンピュータ・ネットワーク上ですべての経済取引がなされるようになれば，電子的な決済手段が必要になると想定した上で，それがクレジットカードや銀行送金のような中央集権的なシステムで実現された場合，中央に位置する主体がすべての経済取引を知り得る立場になると予想した．そのような主体が，個人のプライバシを侵害するBig Brotherになることを彼は危惧した．Big Brotherとは，作家George Orwellが小説『1984年』の中で描いてみせた，監視社会における独裁者の名前である．そこで，中央に位置する銀行が，経済取引が誰によって行われたか把握できないようにするため，現金のように匿名性を持つ決済手段，電子現金（electronic cash）を作るべきだと考えた．

Chaumが想定したネットワーク社会は，彼が論文を書いてから10年後，インターネットの出現によって実現した．彼は，自らのアイディアを実証するため，匿名性を持った電子現金ecashを作り上げ，インターネット上で稼働させてみせた．インターネットの黎明期に出現したこの新しい技術は，興奮を持って受け入れられ，Chaumは一躍，時の人となった．とはいえ，当時のecashは，一部のマニアだけが利用する貧弱なシステムにすぎず，そもそもインターネット上で売買すべき商品もほとんどなかったことから，実用性に乏しいものであった．ChaumはDigiCash社を設立し，実在する銀行でドルと交換可能なecashを発行するなど，プロジェクトの規模を拡大したが，結局，それが社会に受け入れられることなく，1998年にDigiCash社は倒産してしまった．

その10年後，Satoshi Nakamotoはビットコインの原型を提案するペーパーを暗号理論に関するメーリングリスト上に投稿した．2009年1月8日，Satoshiはビットコイン Ver.0.1と称するプログラムを発表する．それ以降，Satoshiと彼を取り巻くネット上のコミュニティに

よって，ビットコインの改良が進められ，取引の実験が繰り返された．Satoshi 自身は，比較的早い段階でコミュニティを離れた．現論文執筆当初から，Satoshi はネット上でのみ周囲と交流し，そのまま姿を消したので，現在でもその正体は不明のままである．しかし，ビットコインのシステムは改良されつつ動き続け，現在では 7 兆円を超す交換価値を持つに至っている．

Chaum と Satoshi の電子現金は，何が違ったのだろうか．電子現金を名乗る以上，Satoshi もまた，プライバシ問題に自覚的であったことは明らかだ．ただし，Satoshi のアプローチは Chaum とは逆であった．Chaum がセンタ・サーバを前提として，特殊なアルゴリズムで利用者の匿名性を守ろうとしたのに対し，Satoshi は P2P 技術を利用することによって，システム全体を「センタを持たない」形とし，安定性を実現するとともに，誰かが独裁者となることを防ぐという対応策をとったのである．よく誤解されるのだが，ビットコイン自体は，匿名性を担保する仕組みは持っていない．むしろ，すべての取引情報をすべてのノードで共有しており，誰もが取引内容を知り得るシステムになっている．Satoshi は，取引で利用されるアドレスを仮名とし，取引参加者の実名が分からないように運用すれば，必要なプライバシは確保されると考えた．

ビットコインの「センタを持たない」という特性は，その後のシステムの発展に大きな影響を与えた．膨大な経済取引を支える決済システムには，高性能なセンタ・サーバが必要だ，というのが，金融業界の常識である．センタ・サーバを安全に維持管理するためには多額のコストがかかり，決済サービスの提供には高額の手数料が必要となる．ところが，ビットコインはセンタを持たず，すべてのノードが同じ情報を共有する．このノードはユーザの安価な PC であり，そのプログラムはオープンソース方式で随時改良が加えられる．このため，中心となる組織が資金や計算機資源を提供しなくても，実用化が開始され，その規模を拡大していくことができたのである．

電子現金システムには，二重使用問題という難しい課題がある．物理的な紙や金属片を手渡しする現金とは異なり，電子現金は電子署名のついた情報であるから，いったん支払いに使用してもその情報は支払った側の手元にも残ることになる．そこで，その情報を使ってほかの者に同じ電子現金を支払うことによって，手持ちの残高以上に支払いを行うことができてしまう．こうした行為が有効に取り締まれなければ，実用可能な電子現金とは言えない．

この問題に対し，Chaum は，センタが取引データを蓄積し，二重使用があった場合のみはその使用者が特定できるような特殊なプロトコルで対応した．これに対し，Satoshi は，「ビットコインの採掘」として知られる特殊な手法でこの問題を解決した．その基本的アイディアは以下の通りである．

Chaum やほかの先行プロジェクトのように，二重使用チェックを行う特定の主体を想定すると，「センタを持たない」という理念と衝突することになる．そこで，取引内容の検証（電子署名の正当性チェックや残高以上に使用していないこと，二重に使用していないことのチェック）についても，誰でも行えるようにした．しかし，たとえば二重使用を行った本人が検証者を兼ね，取引に問題ないと嘘をつくかもしれない．そこで，取引の検証をする際に，一定の作業を行わせ，それだけ計算機資源を投下したことを証明させるようにすれば，その主体による検証を信頼してもよいであろう．このような考え方（Proof of Work，作業による証明）を用いて取引内容のチェックを行い，ハッシュ関数によって連鎖する新しいブロックを生成することを「採掘」と称し，その作業への報酬として，ビットコインを新規に発行して与えるという仕組みを作ったのである．この一連のメカニズムがブロックチェーン技術の原型であり，さらに派生した新しい技術体系を生み出している．ビットコインは，このメカニズムを採用することで，システムの安定運用と取引内容の検証のための資源を，自給自足でまかなうことができるようになった．「センタを持たない」システムが，誰からも資金援助を受けず，2009 年以来，止まることなく長年稼働し続けてきたのは，こうした工夫あってのことなのだ．

この採掘のための「一定の作業」の難易度は，採掘に参加する者の持つ計算能力に応じて自動的に決められる．近年，ビットコインの人気が高まり，大勢が採

掘に参加するようになるにつれて，作業の難易度が増し，膨大な計算能力を持つ専門業者でなければ採掘ができない状態となっている．採掘のために過度に計算コストが必要になると，本来の電子現金システムとしての効率性が失われることには注意が必要である．

図 -1　ビットコインの価格と利用者数

ビットコインの交換価値の推移：経済危機によって相場が高騰

2009 年から実験的な取引を開始したビットコインは，当初は特に注目されることもなく，マニアの間のお遊びとして，ひっそりと続けられた．ビットコインは，ドルや円といった法定通貨で価値を表示せずに，独自の通貨単位 BTC を利用した．歴史的に見れば，ecash の失敗以来，数多くの新規電子現金が提案され，仲間内で実験が繰り返されてきた．その多くは法定通貨建ての電子マネーであったが，中には独自の通貨単位を提案する仮想通貨的なプロジェクトもあった．しかし，ビットコイン以前の仮想通貨は，いずれも短期間で消え去っている．発行主体が法定通貨と同じ価値で買い物等ができることを保証した電子マネーですら，利用者に信用され，受け入れられるには時間がかかった．まして，独自の通貨価値を持つ仮想通貨は，買い物にも価値の貯蔵にも使いにくいので，人々から受け入れられることはなかったのだ —— ビットコインの出現までは．

ビットコインがマニアのお遊びから，実用性のある投資対象として初めて認識されたきっかけは，2013 年 3 月のキプロス危機であった．地中海の小さな島国，キプロスにおいて金融危機が発生し，一時的に銀行が営業を停止した際に，キプロスから資金を海外に移動させる手段としてビットコインが注目され，その相場が 1BTC=200 ドル近くにまで急騰した．危機が収まると相場は下落したが，この事件を境に国際的な資金移動に利用可能という機能が注目され，ビットコインの相場は徐々に上昇していく．2013 年末には中国国内での需要が過熱したことを主因に，一気に 1,000 ドルを超す水準となった．その後，中国人民銀行が銀行口座からのビットコインの購入を禁止したことを主因に相場が半値に暴落，さらに日本にあった世界最大手の仮想通貨交換所，Mt. Gox 社が破綻し，相場は再び 200 ドル近くに下落する．この状態がしばらく続いた後，2016 年ごろから相場は回復を見せ，2017 年に入ってから最高値を更新した後，相場が急騰し，2017 年 8 月時点では 4,000 ドルを超える高値を付けている（図 -1）．

ビットコインの渋滞とその解決策を巡る対立

このように相場が順調に推移する中，ビットコインが仮想通貨として便利に使われていたかというと，そうではない．実際にはビットコインを含む仮想通貨が，「通貨」として利用されている実績はほとんどないのだ．ビットコインの通貨単位 BTC はきわめて激しい価格変動を示している．このため，現段階で商品の販売価格を BTC 建てで表示したとすれば，その価格は時間とともに大きく変動させざるを得ないし，仮に変動させなければ売り手か買い手が損失を被ることになる．収入や支出のほとんどを BTC 建てで生活しているのでない限り，消費者にとっても販売者にとっても，ビットコインを決済手段として利用することはリスクを伴い，不便でもある．

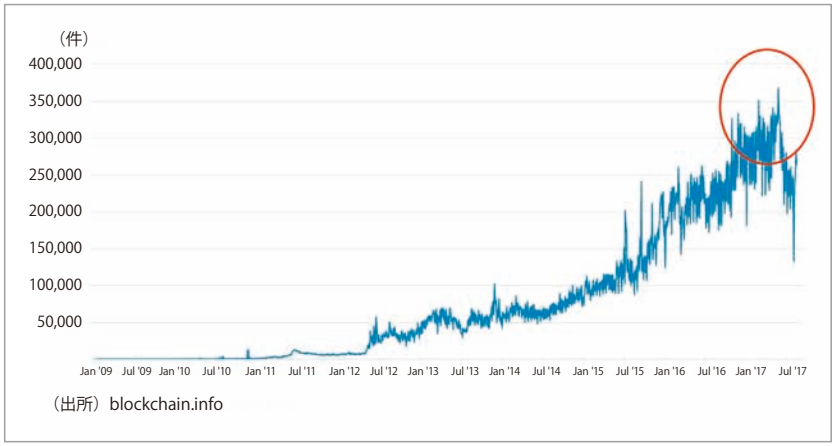

図 -2　ビットコインの 1 日当たり取引件数の推移

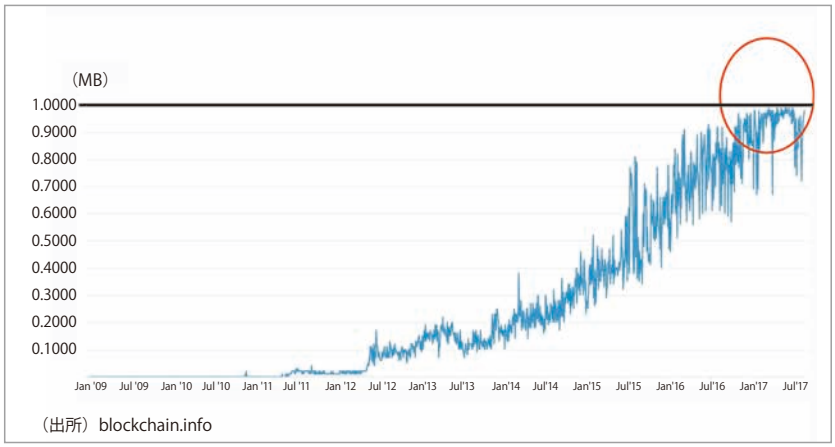

図 -3　ビットコインのブロックサイズの推移

このため，現時点では，ビットコインを取得する目的は，価格上昇を期待した投資目的がほとんどであり，それ以外では，販売店が新規性をアピールするためのデモンストレーションとして BTC での支払いを受け入れているか，限定的な国際的な小口送金手段として利用される程度と考えられている．つまり，ビットコインに代表される仮想通貨は，その名前に反して，「通貨」の基本である「価値尺度」としての機能を果たしてはいないのだ．こうした実態を考えれば，現在の現金や銀行預金などの法定通貨建ての決済手段，貯蓄手段が，仮想通貨に取って代わられるというシナリオを想定するのは現実的ではない．現時点におけるビットコインは，投機対象としてのみ，存在意義を持っているといっても過言ではない．そして，その投機は，将来，ビットコインが法定通貨に代わって日々の資金決済に利用されるかもしれないという淡い期待に基づいている．

ところが，日々の資金決済どころか，そうした期待に基づく投機取引が増加しただけで，ビットコインのインフラが麻痺し，取引が滞るという問題が生じてしまった（図 -2）．元々，ビットコインを売買する際に，取引を起動してから「採掘」が行われ，承認が完了するまでに 10 分程度の待機時間がかかる．ところが，2016 年末頃から，この待機時間が伸びてしまい，取引によっては，何時間も決済が承認されないというトラブルが増えてしまった．

こうしたトラブルが発生した理由は単純であった．ビットコインは，その開発時に，採掘作業の結果生成されるブロックの上限値を 1MB と設定していた．ブロックの中には，ビットコインの取引の内容とそのデータを組み合わせて作り上げたハッシュ値を格納する必要がある．このブロックが平均 10 分に 1 回生成されるのだが，10 分間に発生する取引の数が増えると，ブロックに格納しきれない取引が残ってしまう．このため，承認されずに残ってしまう取引が増えてしまったのだ（図 -3）．

承認遅延の原因が 1MB のブロックサイズの上限値にあることは明らかであり，解決策は限られる．主な解決策は以下の 2 つであった．

① SegWit 導入（ブロック内の冗長な署名データを削除することで，利用効率を倍に引き上げる）
②ブロックサイズの上限値を引き上げる

この問題をビットコイン関係者が議論したが，コア開発者は①を，採掘業者は②を主張し，対立の溝が埋まらなかった．両者の同意を取り付ける前に，コア開発者側が見切り発車的に①を導入しようとし（BIP148 ＝ UASF〈User Activated Soft Fork〉），その期限であった 2017 年 8 月 1 日が「ビットコイン分裂の日」として注目されることになった．しかし，最終的には，8 月 1 日前に妥協が成立し，①と②の折衷案で

ある SegWit2x が採用された. すなわち, 冗長な署名データの削除を実施した上で, 11 月にブロックサイズの上限値を 2MB に引き上げることを改めて投票にかけることに決したのだ. この結果, 危惧されていた 8 月 1 日の UASF による分裂は回避された. しかし, 採掘業者の一部が, ビットコインの新たな分岐から新しい仮想通貨, ビットコインキャッシュ（BCH）を作り出すことを提案し, これが実行された結果, UAHF (User Activated Hard Fork) と呼ばれる分裂が発生した（図 -4）. 具体的には, 8 月 1 日時点で 1BTC を保有していた利用者には, 1BTC に加え, 1BCH がもれなく配布されることとなった. 当初, 分裂による暴落を懸念されていたビットコインの相場は, 8 月中旬現在, 分裂騒動を無難に乗り切ったことが評価されてさらに高騰を続けている.

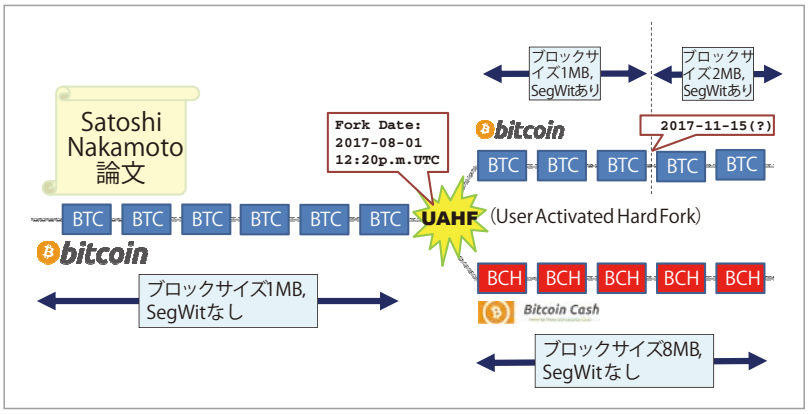

図 -4　分裂後の両ビットコインの仕様

ビットコインの中の人：実は存在した「センタ」

以上が 8 月 1 日のビットコイン分裂問題の経緯なのだが, ここで不思議に思うのは, 本来,「センタを持たない」という理念で, だれもが利用でき, だれもが採掘できるはずだったビットコインにおいて, 何やら内部関係者の覇権争いのようなことが起こっている点である. 実は, 当初の理念は崩れてきており, ビットコインを含む多くの仮想通貨が,「実質的なセンタを持つ」存在となりつつあるのだ. ビットコインのコア開発者や大手採掘業者といった「ビットコインを支える裏方」が存在し, それらの影響力はますます強まっている. センタを持たないからこそ, ビットコインのシステム全体を統治する仕組みも存在せず, オープンソースによるコードのユーザ相互による検証や採掘業者による取引の検証が, システムの安全性を支えると信じられてきた. しかし, ビットコインのエコシステムを支える関係者の影響力が拡大しているとすれば, 現在の不透明なガバナンスの仕組みは, いずれ深刻な影響をもたらしかねない.

もう 1 つ不思議なのは, ビットコインが分裂して新たなコインが誕生し, その流通総額がビットコイン全体の 10% 前後で推移していることである. ビットコインは,「2,100 万 BTC を発行上限とする」ことを標榜し, それが希少性を保証すると考えられていた. しかし, 一部の関係者がシステムを変更したり, 利用者が市場価値を評価することで, 実質的にビットコインの流通量を増加させることができてしまったのだとすれば, ビットコインが将来にわたって希少な存在であり続けるとナイーブに信じ続けることは難しいであろう. こうした懸念は, 現段階ではあまり注目されていないが, 今後を考える上では見逃せない点である.

ICO の急拡大とイーサリアムの高騰

2017 年 5 月以降, ビットコインを含む仮想通貨が急激に値上がりしたのは, 欧米で急速に拡大した ICO（Initial Coin Offering）が原因であるとの見方がある. ICO とは, スタートアップ企業などが仮想通貨を利用したビジネスを立ち上げる際に, 新たなトークンを発行してそれを売却し, 資金調達を行う手段である. 通常の企業の資金調達では, 株式や社債を発行するが, ICO では, 企業が仮想通貨を用いて独自に構築した電子データ（トークン）を販売し, その売上が利益に計上されることになる. このトークンが, 流通市場において高値で売買されることが多いため, 投資家から多

額の資金が集まり，それが仮想通貨市場全体を押し上げる形となっている．こうしたトークンは，仮想通貨イーサリアムの機能を利用して構築されており，その購入にもイーサリアムが用いられることが多い．ICO の拡大により，イーサリアムの相場は大幅に値上がりしている．

ICO 自体はビットコインより後の仮想通貨の新規発行や，仮想通貨の仕組みを利用したプロジェクトにおいて，以前から存在していたものであるが，その規模が急速に拡大したのは 2017 年 5 月以降であり，3 カ月で前年の 10 倍を超える資金調達が行われた（図 -5）．ICO の拡大によるイーサリアムの相場上昇により，その流通総額は，一時，ビットコインとほぼ同じ水準まで上昇した．イーサリアムのみならず，ビットコイン以外の多くの仮想通貨が，ここ半年で急速に値上がりしたため，仮想通貨の流通総額全体に占めるシェアを見ると，この半年で価格が 4 倍に上昇したビットコインのシェアはむしろ低下しており，ひと頃の 9 割前後から 5 割前後で推移している（図 -6）．

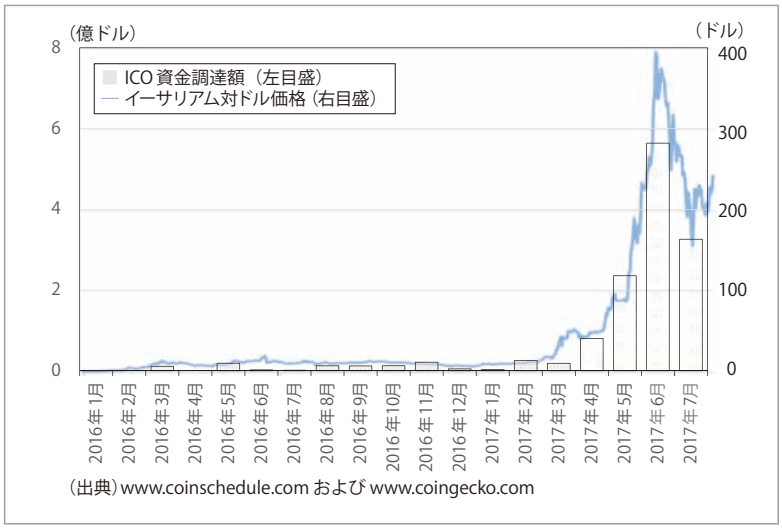

図 -5　ICO による資金調達額とイーサリアム相場の推移

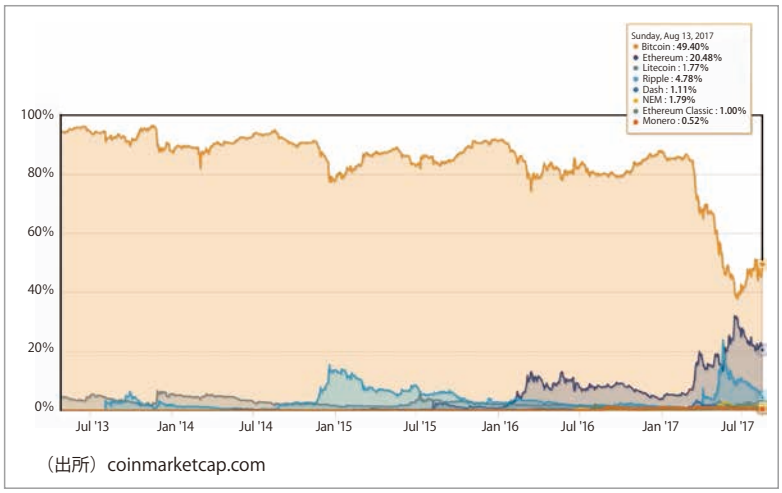

図 -6　仮想通貨の時価総額のシェア

ICO は，巨額の資金が短時間に匿名で取引されることから，資金洗浄やテロリストによる資金調達の機会を増やしかねないことが指摘されている．また，トークンの設計次第で，各国の証券法の対象とされた場合，証券法制における開示規制や行為規制の対象となり得るとの指摘もある．このため，各国で ICO の規制に関する議論が活発に行われている．

こうしたさまざまな課題を抱えつつ，ビットコインやその他の仮想通貨は，投資対象として裾野を広げつつある．その動向については，今後も注視していく必要があるだろう．

参考文献

1）Nakamoto, S. : Bitcoin : A Peer-to-Peer Electronic Cash System.
2）Chaum, D. : Blind Signatures for Untraceable Payments, Advances in Cryptology Proceedings of Crypto. 82.

（2017 年 8 月 16 日受付）

岩下直行　iwashita.naoyuki.7e@kyoto-u.ac.jp

1984 年慶大・経済卒業．同年日本銀行入行．2005 年金融研究所・情報技術研究センター長，2014 年金融高度化センター長，2016 年 FinTech センター長．現在，京大・公共政策大学院教授．