# なぜいまフィンテックとブロックチェーンが注目され，これからどう社会を動かすのか

応般

楠 正憲（国際大学グローバル・コミュニケーション・センター）

## なぜいまフィンテックが注目されているのか

### ◈ 再び脚光を浴びるフィンテック

さまざまなカンファレンスが開催され，専門誌が創刊されるなど，このところフィンテックへの関心が高まっている．フィンテックとは Financial Technology の略で，元々金融分野での IT 利活用全般を指していたが，ここ数年は特にインターネットで新たな金融サービスを提供するスタートアップのことを指す場合が多い．

元々日本における商用電子計算機の活用が 1955 年の東京証券取引所と野村證券による UNIVAC120 導入から始まったことからも明らかなように，金融機関は歴史的に電子計算機の先進ユーザだった．今日の金融機関にとっても情報システムは事業継続のために必要不可欠な基盤となっている．にもかかわらず，なぜ最近になってフィンテックが脚光を浴びているのだろうか．

Google Books n-Gram Viewer（図 -1）によると Financial Technology という用語は 1960 年代前半から使われ始めた．1964 年の東京オリンピックで電子計算機の有用性が実証され，日本で勘定系オンラインシステムが構築され始める少し前にあたる．略語のフィンテックは 1980 年代前半から使われたが，これは当時レーガノミクスによる NASA などの政府研究機関が縮小され，数学に長けたロケットサイエンティストたちが金融業界に流れ込んだ時期にあたり，金融派生取引や裁定取引，アルゴリズム取引など，計算機があって初めて実現できる金融工学の隆盛と重なっている．いずれも 1990 年代に入ると一般化すると同時に限界や弊害も明らかとなってブームは収束し，フィンテックという用語は書籍では 21 世紀に入ってからはデータの取得できる 2008 年まで，ほとんど使われていない．

フィンテックへの関心の停滞が大きく変わるのは 2013 年末，日本では 2015 年に入ってからのことだ．Google Trends（図 -2，3）で検索クエリの検索頻度をみると，全世界では 2013 年 11 月に小さな山があり，2014 年に入ってから大きく伸びている．英 Economist 誌[☆1] は 2015 年 5 月に“The Fintech Revolution”という記事を掲載し，2013 年に約 40 億ドルだったフィンテック分野への投資が，2014 年には 3 倍の 120 億ドルに膨れ上がったことを報じている．いったいなぜ 2014 年に入ってから再び急激にフィンテックへの関心が高まっ

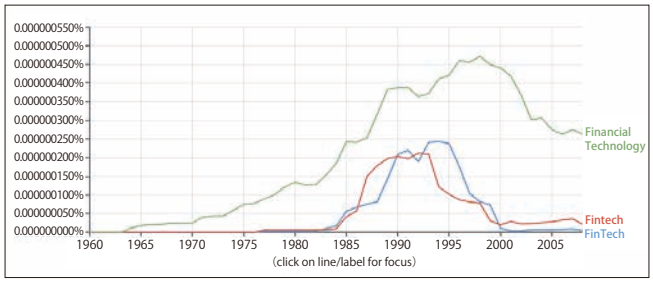


図 -1　Google Books n-Gram Viewer による Fintech の出現頻度の推移

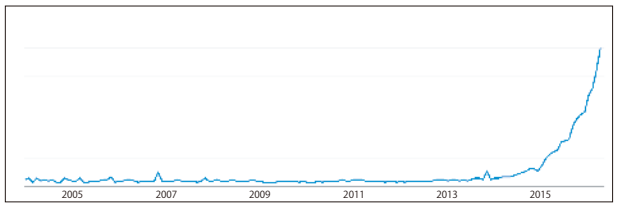


図 -2　Google Trends による Fintech の検索頻度の推移（全世界）

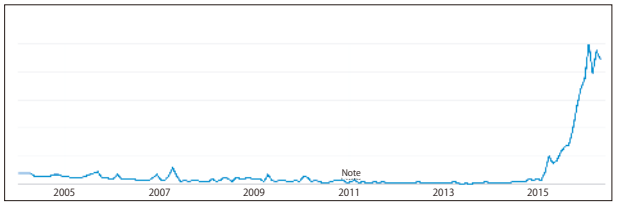


図 -3　Google Trends による Fintech の検索頻度の推移（日本）

☆1 http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution

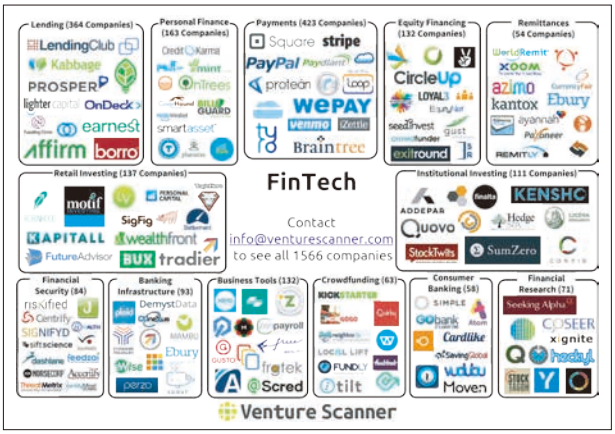


図 -4　米国のフィンテック・カオスマップ
出典 : https://www.venturescanner.com/


図 -5　日本版フィンテック・ベンチャー業界マップ
出典 : http://www.emreyuasa.com/

たのだろうか．

既存金融サービスの IT 化は不発だったが IT を前提とした新たな金融サービスは成長を始めた．

オンラインバンキングを始めとして金融サービスのインターネット対応はインターネットの商業利用が進んだ 1990 年代末から漸進的に進んできた．これらのサービスの API 化やデータフォーマットの標準化も同時期から進んでいたにもかかわらず，脚光を浴びることもなかった．オンラインバンキングも 2000 年代前半までは OFX（Open Financial eXchange）という金融情報交換のデータフォーマットによる家計簿ソフトとの連携などを売りにしていたが，いつの間にか姿を消し，推進していたマイクロソフトも家計簿・資産管理ソフト市場から撤退した．

第一次フィンテックブームで既存の金融機関が IT を使って投資のパフォーマンスを高め，顧客サービスの改善を図ったのに対して，2013 年末からの第二次フィンテックブームの特徴は新規参入が増えている点である．寡占市場での競争要素としてのフィンテックではなく，新たな企業が IT を前提とした金融サービスを提供し始めたのだ．

## ◈ 続々と生まれる振興企業

フィンテックとして括られる分野の新興企業は，米 Venture Scanner 社のまとめた概要（図 -4）によると，貸し出し，個人資産管理，決済，株式による資金調達，送金サービス，リテール投資，産業投資，セキュリティ，銀行基盤，業務支援，クラウドファンディング，消費者向けバンキング，金融調査などの分野に大別できる．グロービスキャピタルパートナーズの湯浅エムレ秀和氏は，日本国内でほぼ同様の整理を行っている．金融は伝統的に信用と顧客基盤，資金力を必要とする分野で，新規参入が難しい．なぜこのタイミングでフィンテックスタートアップによる金融分野への新規参入が可能となったのだろうか．

スマートフォンの普及によってアプリケーション市場が活性化するとともに，事業者が利用者の位置情報をはじめとしたさまざまなデータを取得できるようになったことで，これらを活用した新たな金融サービスを立ち上げるベンチャー企業が相次いだ（図 -5）．

しかしながら特に 2014 年に入ってベンチャーキャピタルがフィンテックに注目した理由は，そうしたサービスの多様化だけで説明することが難しい．スタートアップが既存の巨大金融機関にはできなかった目新しいサービスを提供するだけでなく，今ある管理通貨制度や銀行システム，決済インフラを置き換えかねない技術革新として，暗号通貨のビットコインに関心が集まった時期と重なっている．

NCSA Mosaic を開発し，Netscape を創業して AOL に売却後，ベンチャーキャピタルとなった Marc Andreesen 氏は，2014 年 1 月ビットコインについて New York Times に寄稿し「PC にとっての 1975 年，インターネットにとっての 1993 年，そして 2014 年にはビットコインがくると私は信じ

る」と評した．金融と同様に元々資本力と顧客へのリーチが重要だった通信業がインターネットで激変した波を革命の旗手たちは，ビットコインがお金のインターネットとなって金融業界に破壊的イノベーションをもたらすことに賭けているのだろうか．

## 第二次フィンテックブームの端緒となったビットコインバブル

ビットコインは 2008 年に Satoshi Nakamoto を名乗る者による論文がメーリングリストに投稿され，翌 2009 年初頭から運用され始めた．当初は好事家同士で Web サイトの構築を請け負うなどの原価のかからない役務取引から使われ始めたが，早々に現金との相場が成立した．実際に商品の売買が行われたのは 2010 年 5 月，フロリダ州のビットコイン愛好家が，10,000 ビットコインでピザ 2 枚を買うと書き込んだところ，数日後に実際に配達されたのが最初とされている．

初期のビットコインを支えた Cypherpunk と呼ばれる暗号を愛好するプログラマは，国家権力に対して根強い不信感を持っている．コミュニティの中では中央銀行による裁量的なマネーサプライの管理よりも，アルゴリズムによる機械的な通貨発行量の管理を行った方が，長期的には価値を維持できるという信念が語られがちだ．当時米国ではサブプライム・ローン問題から派生した金融危機に対応するため QE1 と呼ばれる量的緩和策で 1 兆 7,250 億ドルが供給された時期で，大規模な量的緩和が長期的な貨幣価値に与える影響が懸念されていた．

ビットコイン愛好家同士によるピザの売買から約半年後の 2011 年 2 月，ノードの IP アドレスを隠蔽して匿名通信技術 Tor（The Onion Router）を利用した匿名サービス上で，違法ドラッグや児童ポルノ，クレジットカード番号などさまざまな違法取引を仲介するブラックマーケット“Silk Road”が立ち上がり，売り手も買い手も匿名での取引を望み，クレジットカードや銀行振込を使えない違法取引の決済手段としてビットコインが利用されるようになった．

2013 年 3 月，米国財務省でマネーロンダリング対策を担当している組織である FinCEN（Financial Crimes Enforcement Network[☆2]）は，ビットコインが資金洗浄に悪用されないよう仮想通貨の取引所運営・利用に対するガイドラインを発表した．このガイドラインでは，仮想通貨の利用そのものは現実として受け入れた上で，取引所に対しては口座開設時に本人確認の義務を課すこととした．このことは既設のビットコイン取引所にとって規制強化となるが，裏を返せばこれまで法的リスクを見積もることの難しかったビットコインについて，米国当局が事実上のお墨付きを与え，事業リスクを見積もりやすくするきっかけとなった．

2013 年 3 月，欧州ユーロ圏に属する小国キプロスは財政破綻に直面し，10 万ユーロ以下の預金には預金残高に対して最大約 10% の税をかけると発表した．預金の引き出しや送金は一時的に凍結されたが，ビットコインに変えれば課税を免れるということで初めて法定通貨から仮想通貨への逃避が現実のものとなり，3 月初旬には 40 米ドル弱だったビットコイン価格が 4 月には 200 米ドルを超える水準まで跳ね上がった．キプロスでは国立大学の学費を始めとして，さまざまなものをビットコインで支払えるようになった．一時的・局所的ではあるがユーロ建て預金よりもビットコインの方が安全な資産となった瞬間だ．

Silk Road は 2013 年 7 月 23 日に構成するサーバが FBI（米連邦捜査局）によって押収され，10 月 2 日には摘発されて広く一般に知られるようになった．このサーバに残っている記録によると，Silk Road は 2011 年 2 月 6 日から 2013 年 7 月 23 日の間に，146,946 の買い手，3,877 の売り手の間で約 1,229,465 件の取引を仲介し，9,519,664BTC（BTC：ビットコインの通貨記号）の流通総額から 614,305BTC の仲介手数料を得たとされる．この仲介手数料は日本円に換算してピーク時に 600 億円以上，執筆時の相場（2016 年 5 月）でも約 300 億円以上にあたる．

FBI による Silk Road の摘発を通じてビットコインについて知る人が増え，ビットコインバブルは加熱した．

☆2 https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

摘発の発表時には 130 ドル周辺だったビットコインの取引価格は Silk Road の摘発で一時は 90 ドルを割る水準まで暴落したが，1 週間も経たないうちに元の価格に戻し，11 月末の時点では 200 ドルを超える水準まで上昇，11 月末には 1,100 ドルを超える水準まで暴騰した．しかしながら 12 月に入って中国人民銀行がビットコインに対する規制を発表したことで，ビットコインの価格は半値以下に暴落した（図 -6）．外国為替を厳しく規制している中国において，ビットコインの採掘☆3 は合法的に資産を海外へと移転する数少ない方法の 1 つとなっており，いまや採掘者のシェアの 8 割以上を中国本土が握っている．2014 年 3 月には，2013 年まで世界最大規模のビットコイン取引所だった MTGOX(本社：東京渋谷）が破綻し，ビットコインの法的位置付けについて，日本でも活発に議論されるようになった．

図 -6　2013 年 10 月から 12 月にかけてのビットコインの値動き（出典：BitcoinCharts, BitStamp）
This chart is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.
http://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2013-10-01zeg2013-12-31ztgSzm1g10zm2g25zv

## ビットコインの神話とブロックチェーンの現実

一連の 2013 年に起こったビットコインバブルは非常に多くの金融関係者や起業家が暗号通貨の可能性を見出す契機となった．真っ先にビットコインで置き換えられそうな swift（国際銀行間通信協会：Society for Worldwide Interbank Financial Telecommunication）など国際決済基盤を支える大物らが相次いでビットコインベンチャーを立ち上げた．ビットコイン界隈は気難しい夢想的な Hacker の砂場から，海千山千のギラギラした金融屋の鉄火場へと一変したのである．

しかしながら投機や資本逃避目的での保有や，違法取引や資金洗浄といった脱法的な使途，決済インフラの整わない新興国での送金などを除くと，ビットコインの事業開発は厳しい状況が続いている．まだ各国が仮想通貨についての法制を整備しているところで，今後の方向性によっては事業への影響が大きい．日本では，反マネーロンダリング規制や利用者保護の規定が不明確であったが，法改正により，交換業者について，これらの規定の適用が明確化された．消費税の扱いなど，まだクリアされていないが事業への影響が大きい論点も残っている．

また先進国の小口決済で実際にビットコインを使おうとすると，スケーラビリティやプライバシーが大きな課題となる．現状のビットコインネットワークで 10 分ごとに処理できるトランザクションの容量は 1MB 程度に制限されており毎ブロック 1,000 ～ 1,500 取引しか記録できない．これは平均すると毎秒数件という非常に少ない件数で，先進国の小口決済で使われ始めると一瞬で行き詰まってしまう．本来ソフトウェアの改修によって技術的には容易に修正できる課題だが，ビットコインの運営に多額の資金や利害関係が絡むがゆえにコンセンサスの形成には時間を要しており，2015 年夏に 1MB のブロックサイズを 2016 年から 8MB に拡張し，その後，約 2 年ごとにブロックサイズを倍にする Bitcoin XT という処理容量を改善した新たな仕様が提案されたものの，実現しなかった．その後も議論はスケーリング・ビットコイン・ワークショップで続けられ，まずは現行のブロックサイズを維持しつつ，より効率的に取引を記録する手法などが議論されている．

もう 1 つビットコインを小口決済で利用しようとした場合に問題となるのがプライバシーだ．ビットコインの原論文はユニークなプライバシーモデルを提唱している．銀行などのシステムでは利用者の個人情報と紐付く取引履歴や預金残高は，アクセス制御によって正当な権限を持った者しかアクセスできない．しかしながらビットコインでは取引はすべてブロックチェーン上に記録されて全世界に公開されている．取引履歴をすべて公開

☆3　ビットコインの取引を処理するために必要な計算処理で，最初に問題を解いた者が報酬を得られる，詳しくは後述．

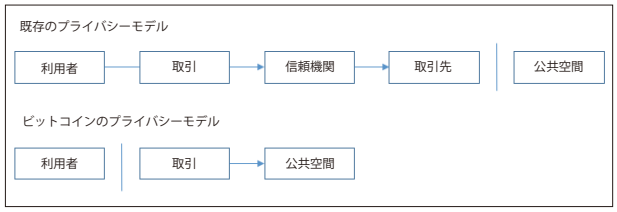


図 -7　ビットコインのプライバシーモデル
出典：Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto 2008 を元に作成

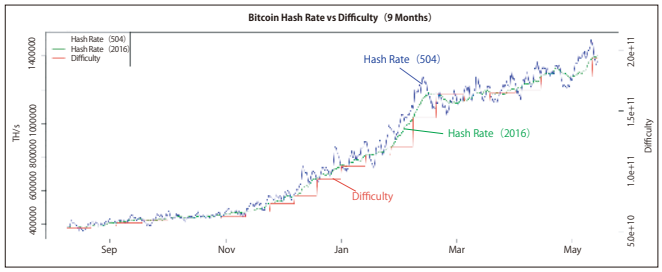


図 -8　ビットコインのハッシュレートとディフィカルティの推移
出典：BitcoinWisdom

する代わりに，本人確認を要さず，自由に銀行口座にあたるビットコイン・アドレス（キーペアのハッシュ値）を作成でき，そのアドレスと利用者の個人情報が結びついていない範囲において，プライバシーが確保されるという考え方である．現実に違法取引などに利用されていることからも分かるように，大量にアドレスを生成して使い分け，ミキシングサービスなど多数の取引を混ぜ合わせることで追跡性を制限する仕組みを使うことでプライバシーを確保できる．しかしながら普通にビットコインを取引に用いる限りにおいて，送金相手は自分のビットコイン・アドレスを知ることができ，そのビットコイン・アドレスの残高や，過去の取引相手と金額は，すべてブロックチェーンを通じて全世界に公開され簡単に追跡できる．一般の電子マネーと異なり，プライバシーを守りながらビットコインを使うには，非常に高いリテラシーを要求される．

ビットコインの優れているとされている点として，P2P で利用者の計算機資源を活用することで低廉なコストで運用できることが挙げられる．ビットコインの安全性は約 10 分ごとに解が見つかるように調整された採掘と呼ばれる計算によって担保される．採掘とは Proof of Work と呼ばれる特定の条件を満たした nonce を求めるハッシュ値の計算，ネットワーク全体の計算能力（ハッシュレート）に応じて難易度（ディフィカルティ）を調整する仕組みである．

集権的な鍵管理ではなく，採掘を無数の利用者間の計算競争によって台帳にタイムスタンプを押すことで，運用者がなくても機能するように設計されている．この仕組みは単独のビットコインを運用する上では機能するが，後追いで似たようなものをつくろうとしても，安全性を担保するには乗っ取られないだけの計算能力を運用する必要が生じる．

こうした問題を回避しつつビットコインのアーキテクチャの恩恵を受けようとする流行がブロックチェーンだ．元々ブロックチェーンはビットコインの取引記録を保存するデータ構造を指していたが，派生してビットコインから影響を受けた分散台帳管理技術を総称してブロックチェーンと呼ぶ場合が多い．ビットコインの仕様を拡張してほかの財産的価値を扱えるようにした Open Asset Protocol や，Proof of Work に代わるアルゴリズムを用いることでビットコインよりも高い拡張性と性能を実現した仕組みがある．これらの技術はビットコインの実績を背景に，低コストで無停止の安全な取引を実現すると主張しており，さまざまな実験が行われているところだ．しかしながらビットコインの仕組みを離れてブロックチェーン技術が機能するかどうかは検討を要する．

まずビットコインの運用には費用がかかっているものの，誰も負担せず通貨発行益を充当している．これは無から生まれた通貨発行益を山分けできるビットコインだからこそ実現できているが，ブロックチェーンを商用利用する場合には運営主体が採掘費用を負担する必要が生じる．またビットコイン自体は正確な分散トランザクションを正確に処理する仕組みを持っているわけではなく，ビットコインのブロックチェーンに記録された価値こそが現実であることを受け入れるルールの元で，通貨の発行量を制御し，二重利用を防止しているに過ぎない．

通常の取引のように，情報システム上の値ではなく法律上の貸借関係が原本となる一般の情報システムでは，現実とブロックチェーン上の記録が食い違うことは障害として認識される．ビットコインが数百億円の価値を管理してきた信頼できる実装であることと，それをビ

ットコイン以外に使って適切に機能するかどうかはまったく別の問題である．ビットコインは三式簿記の採用をはじめ，データ層の信頼性が低くてもデータの一貫性が保たれるようさまざまな工夫を凝らしているが，ほかの使途でブロックチェーンを用いるには，そういったデータ構造上の工夫を個別に考える必要が生じる．

もちろん改竄防止機構を備えた分散台帳を一から設計することと比べれば，ブロックチェーンのミドルウェア上で台帳を構築する方が容易ではある．P2P 通信，データ構造，暗号アルゴリズムの使い方など，ブロックチェーンの作法を真似ることによって解決できる課題は少なくない．とはいえブロックチェーン上でサービスを構築したからといって，低廉な価格で大規模分散システムを構築できるとは限らない．ビットコインはブロックチェーンの欠点を知り尽くした開発者自身が，その欠点を補うように上位のデータ構造や運用ルール，エコシステムを設計しているからこそ機能しているのであって，要素技術の 1 つに過ぎないブロックチェーンだけを切り出して汎用化しようにも同様には機能しないだろう．

## ブロックチェーンはフィンテックに何をもたらすのか

ブロックチェーンが金融の世界に革新をもたらすかは未知数だが，フィンテックに投じられる多額のシードマネーの一部がブロックチェーンに投じられつつある．これは大手ベンダによる寡占で消費者向けサービスと比べて資本投下の少なかった企業向け暗号ライブラリや分散処理ミドルウェアの新技術を商用化する上で，晴天の慈雨となるのではないか．

ビットコイン自体は運営主体を持たない暗号通貨のコンセプトを実証する試作として大きな成功を収めたが，汎用的な分散データベースとしては暗号アルゴリズムの使い方やトランザクション処理の仕組みとしては未熟で，学術的なレビューと改善を必要としている．前述したパブリック・ブロックチェーン（インターネット上で公開され，自由にアクセスできるブロックチェーン）の抱えているプライバシーの問題も，これまで学術的には活発に研究されながら，需要を見出せず商用化されずにきた高機能暗号を実用化する上では突破口となるかもしれない．

そして何よりきわめて保守的で数十年の設計負債を抱えている金融機関間のネットワークに対しては破壊的イノベーションをもたらす可能性がある．この分野では元々各ノードで取引が適切に処理される前提で，紙の時代からの業務フローを，電文に置き換えるように設計されてきた．それぞれ個別に設計された情報システムを相互接続し，組織間の業務を電子化するために作られた通信手順に過ぎず，ノードを超えてシステム全体としてのデータの一貫性や取引の成立を担保するという発想ではつくられていない．

システム間の接続にブロックチェーンの採用を検討することは，それぞれのノードで共通のミドルウェアを動かし，単にプロトコルを揃えるのではなく，系としてデータの一貫性や取引の実行を担保する仕組みを構築することとなる．これまで多くの金融情報システムや決済ネットワークは，所与の業務要件ありきの設計に基づいて電子化されてきた．いまフィンテックとして擡頭（たいとう）しつつあるビットコイン取引所やブロックチェーンを使ったシステムは，まず所与のものとしてネットワーク全体のアーキテクチャがあって，その上にどう業務を乗せていくかという発想でつくられている．

それぞれの金融機関が接続するかどうか懐疑的な見方もある中で，日銀ネット（日銀と銀行間のオンライン処理システム）は 2015 年から稼働時間を延長し，全銀システム（銀行間のオンライン処理システム）は 2018 年には 24 時間送金を実現すると発表した．金融 API を使ったサービス間連携やブロックチェーンの実証実験など，金融機関とフィンテックスタートアップの協業も進みつつある．

金融領域では設計負債を溜め込んできたシステムが少なくない．ブロックチェーンへの関心の高まりが，歴史的経緯にとらわれずにアーキテクチャやサービスを見直す契機となることを期待できるのではないか．

（2016 年 6 月 2 日受付）

楠　正憲（正会員）■ kusunoki@glocom.ac.jp

インターネット総合研究所，マイクロソフトを経て 2012 年ヤフー入社．現在は CISO-Board として情報セキュリティー対策に従事．2011 年から内閣官房番号制度推進管理補佐官，2012 年から同政府 CIO 補佐官に任用．