日中資本市場ラウンドテーブル
【新技術革命と金融産業の進化】

2018年6月30日

日本におけるFinTechと仮想通貨を巡る最新動向

京都大学 公共政策大学院 教授
PwCあらた有限責任監査法人 スペシャルアドバイザー

岩下 直行

目次

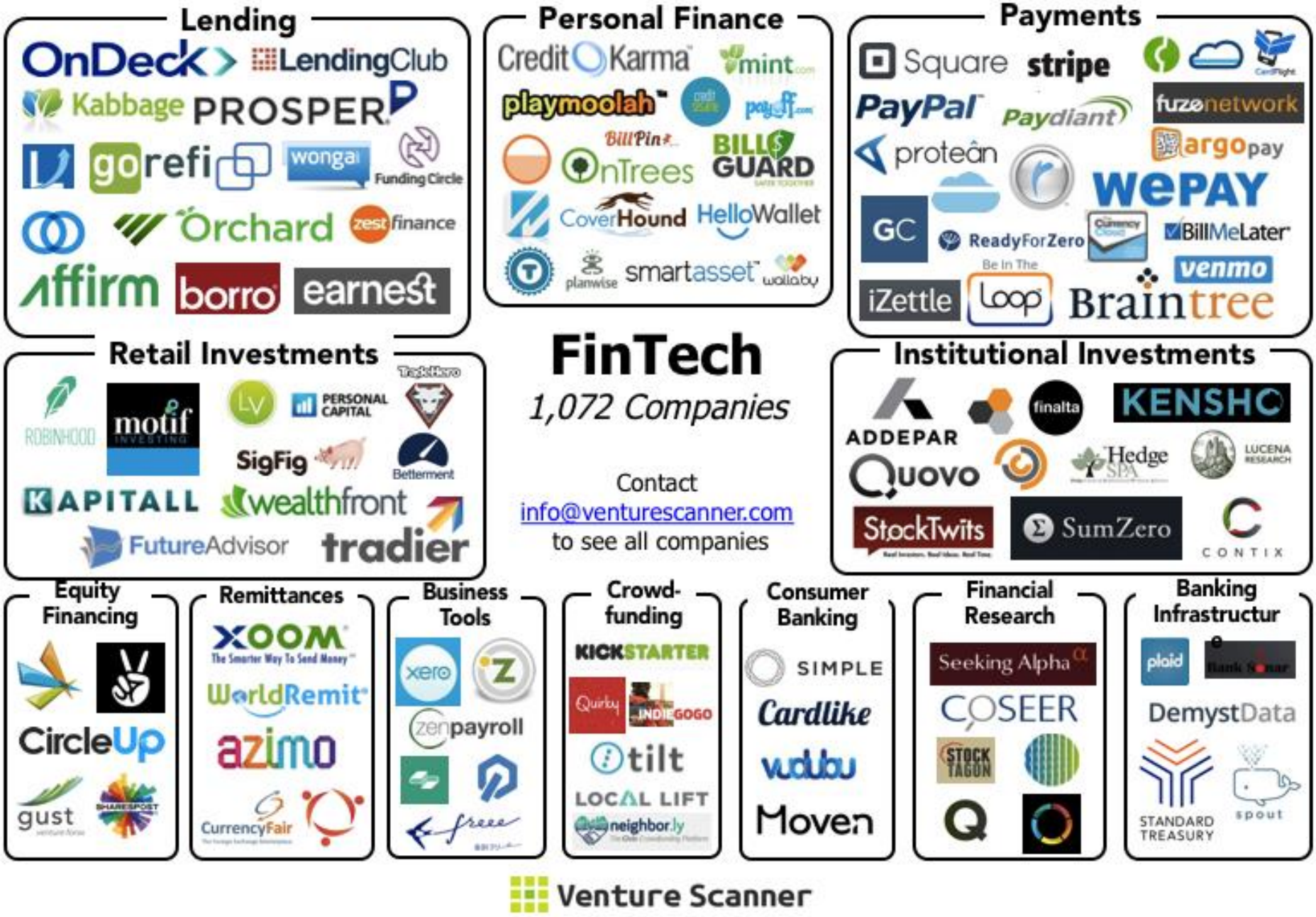
【FinTech編】
1. シリコンバレーからの挑戦者～FinTech企業の勃興
2. 日本の金融機関に期待される対応
3. インターネットバンキング　～FinTechの前提条件
4. 金融オープンAPI　～イノベーションの次のハードル
5. 新興国におけるキャッシュレス化進展の影響

【仮想通貨編】
6. 仮想通貨の暴騰と最近の乱高下
7. ICOの増加と仮想通貨の高騰の背景
8. コインチェック事件と取引所セキュリティ
9. 中央銀行デジタル通貨を巡って
10. 金融庁における検討作業の進捗

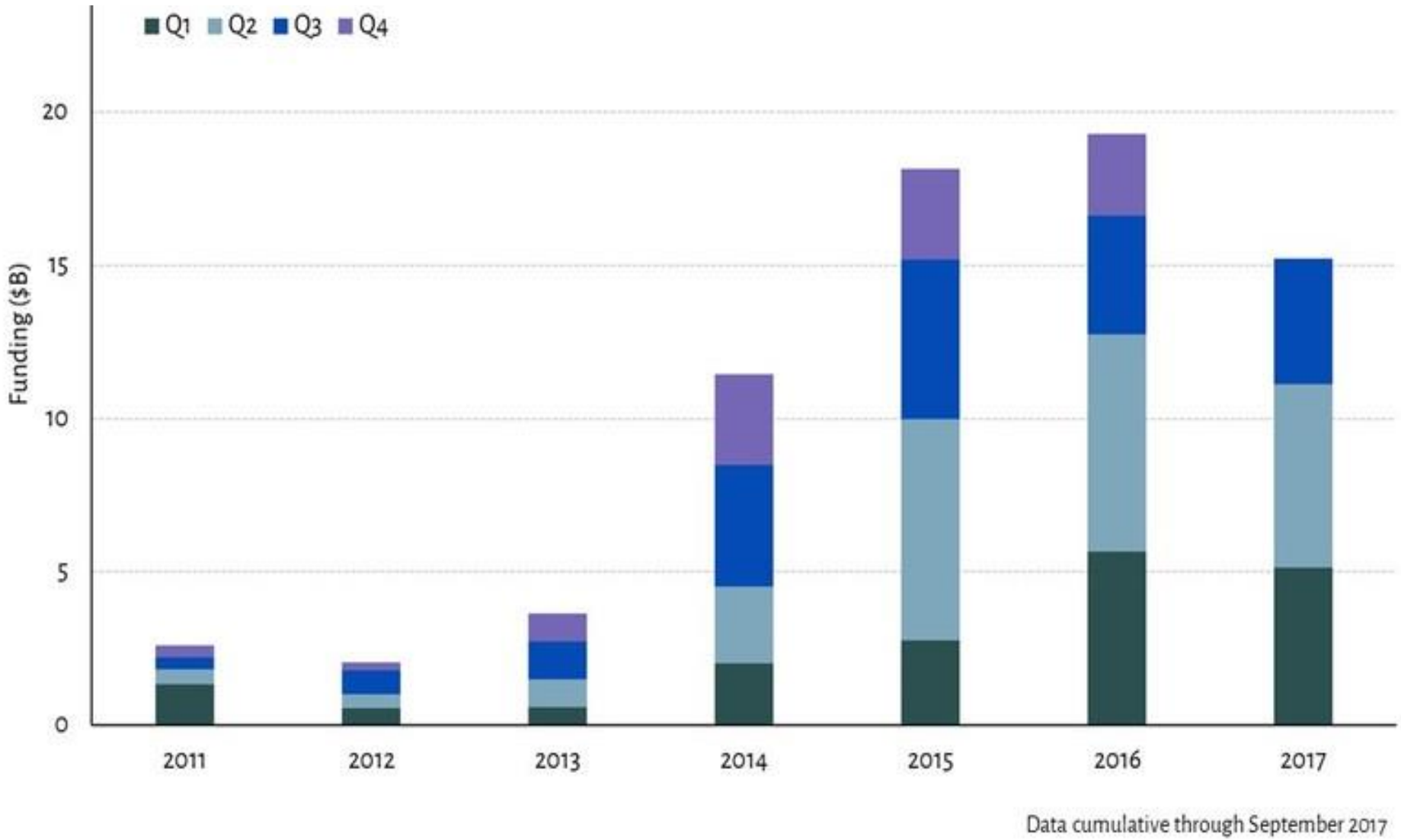
【FinTech編】

1. シリコンバレーからの挑戦者
～ FinTech企業の勃興

シリコンバレーから様々なFinTech企業が勃興している



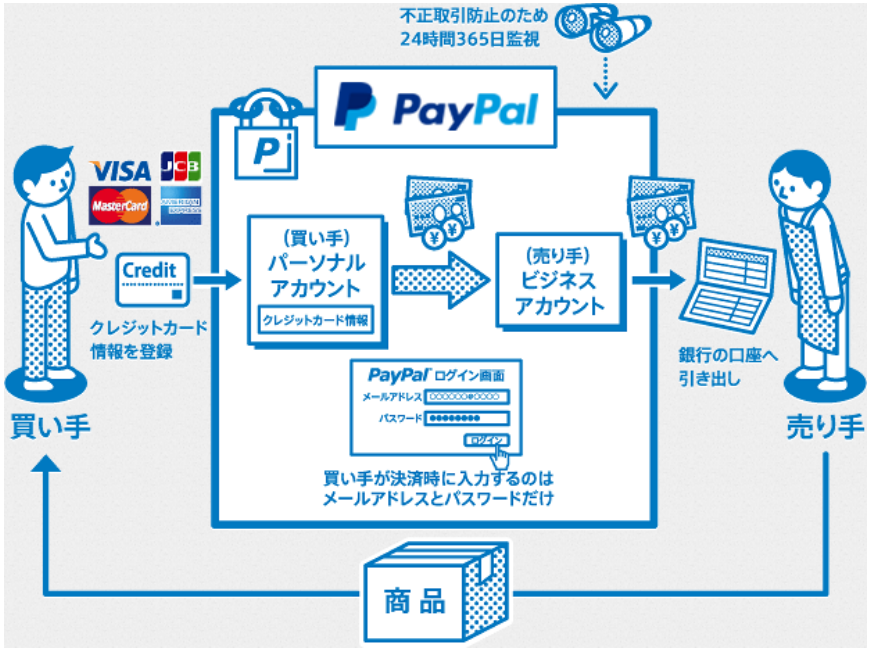
世界のFinTech投資額の推移

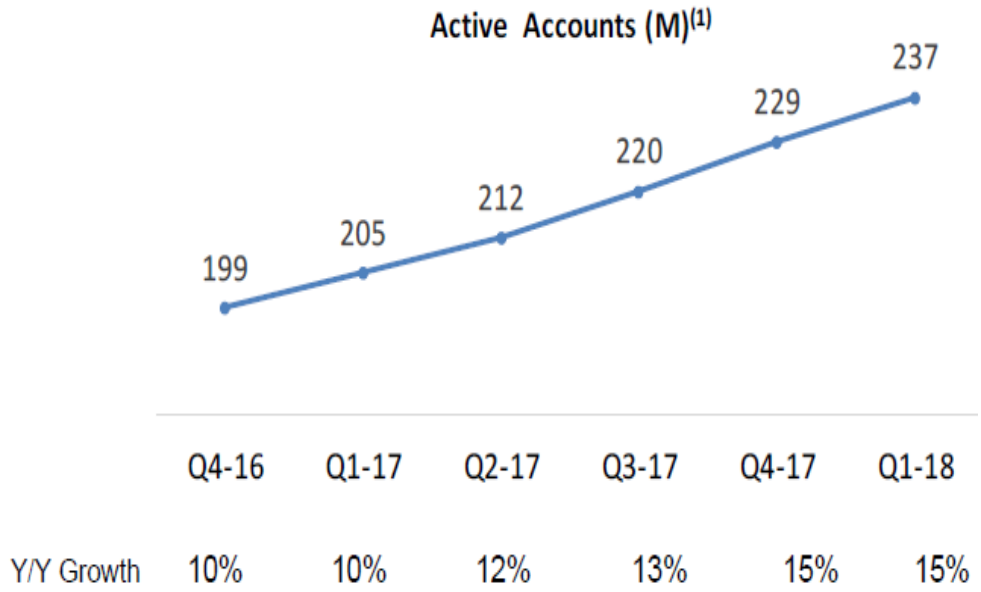


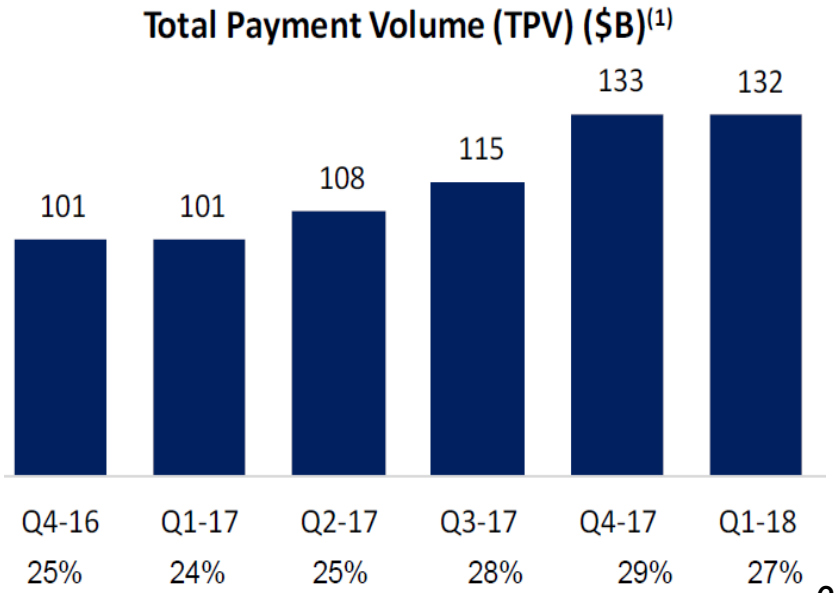
PayPal による銀行業の「再発明」

PayPal は1998年設立。FinTech企業の中では最古参であり、既に世界202か国、25通貨において、2億3700万口座が利用されている。

PayPal の強みは、自らが金融機関間を接続するネットワークインフラや端末機器を持たず、全てをインターネット上で構築している点にある。伝統的な金融機関がシステムインフラの維持管理に膨大な費用を投じているのに対し、PayPal はコスト面で圧倒的に有利な立場にあり、金融業界の深刻な脅威と受け止められている。こうしたことから、PayPal は「インターネットを利用して銀行業を再発明した企業」とも描写される。







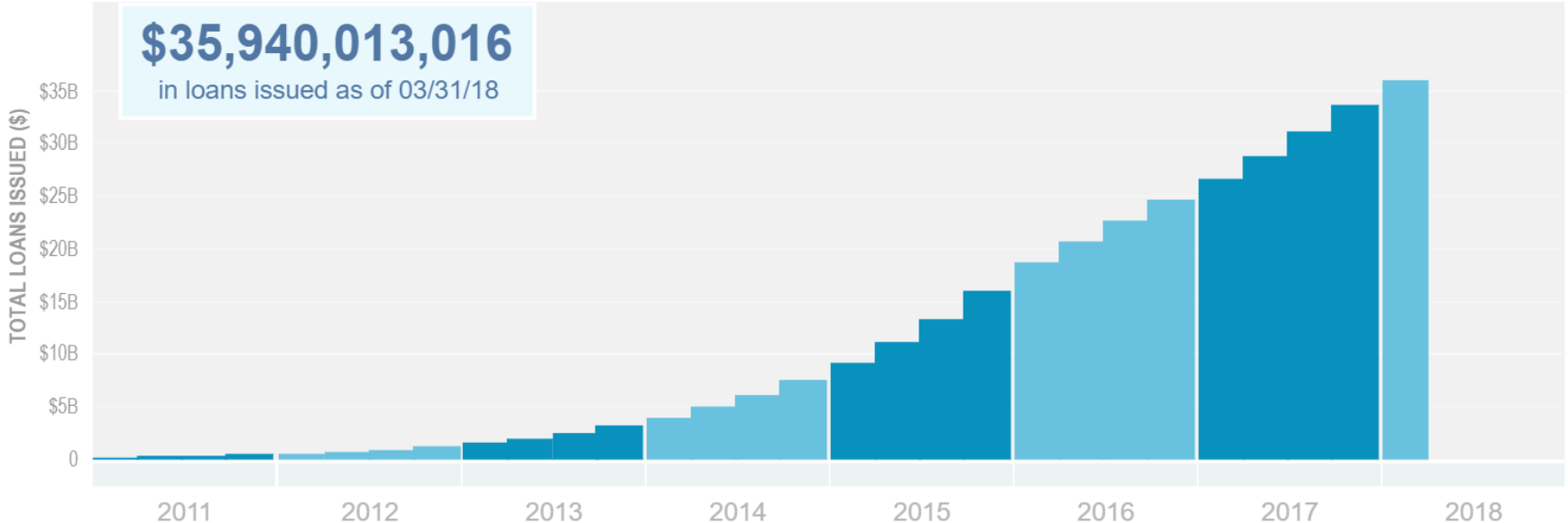
Lending Clubによる新しい融資の形態

Lending Clubは自ら融資を行うのではなく、貸し手と借り手とをマッチングさせて手数料を稼ぐビジネス。マーケットプレイス・レンディングと呼ばれる。こうしたマッチングで組成された融資の累積額は、2018年3月末で4兆円近くに達している。

Fair Isaac社が提供する信用評価システム（FICOスコア）をベースに、貸出金利が設定されている。

伝統的な金融機関が果たしていた役割を奪う、典型的な「中抜き」（disintermediation）ビジネスであり、個人向け融資の分野では、銀行の強力なライバルになりつつある。

Lending Clubの累積取扱額の推移



金融分野におけるビジネスモデルの実験場としてのFinTech

インターネットがなかった時代 （Before Internet）	事業者が通信プロトコルや端末仕様を定め、システムインフラから業務プログラムまで全てを設計して構築。	莫大な費用が必要であるため、大企業が精緻な事業計画を立てて長期プロジェクトを遂行する必要。
インターネット後の時代 （After Internet）	事業者自らが標準やインフラを構築するのではなく、インターネット上で安価に提供されるシステム基盤を利用することが可能に。	莫大な費用も精緻な事業計画も必要なくなるため、小規模なベンチャー企業が様々なビジネスのトライアルを行うことが容易に。

２．日本の金融機関に期待される対応

現在の金融ITの課題

① 金融業界は1970年代からIT化に取り組み、ITを重要な経営資源と位置付けてきた。しかし、金融機関の業務の現場では、「本来ITが持つ力が十分に発揮されていない」という指摘が多く聞かれる。

② 現在の金融ITは、堅牢性や高度な可用性を誇るが、半面、柔軟性に乏しく、維持管理や制度対応に多大なコストと時間を要する。その結果、本来イノベーションの手段として利用されるべきITが、むしろイノベーションを阻害する一因となっている、との声もある。

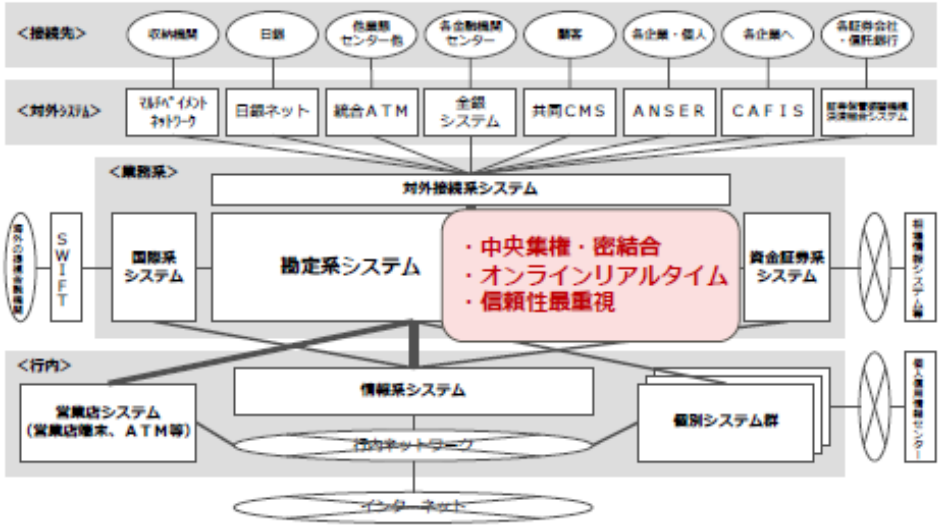
③ 現在では主流とは言えない技術体系に依存する勘定系システムにかかるコストを節約し、主流となった新しい技術体系の活用に経営資源を投じることが必要である。

④ IT投資を戦略的に進めるにあたり、顧客の利便性向上のために必要な技術は何かという観点から検討を深める必要がある。

同じくレガシーを抱えていても大違い

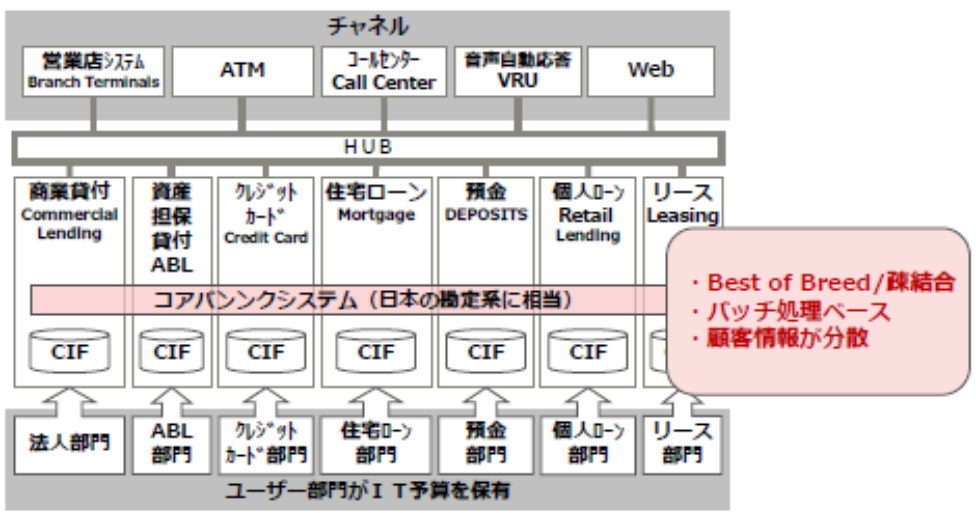
日米の金融ITの基本構造の差異

現在の銀行システムの全体像と特徴



日本の銀行の情報システムは、勘定系システムを中心に**密結合**しており、システムの一部の変更が全体に影響するため、変化への対応が遅れがちであった。

米銀の基幹システム



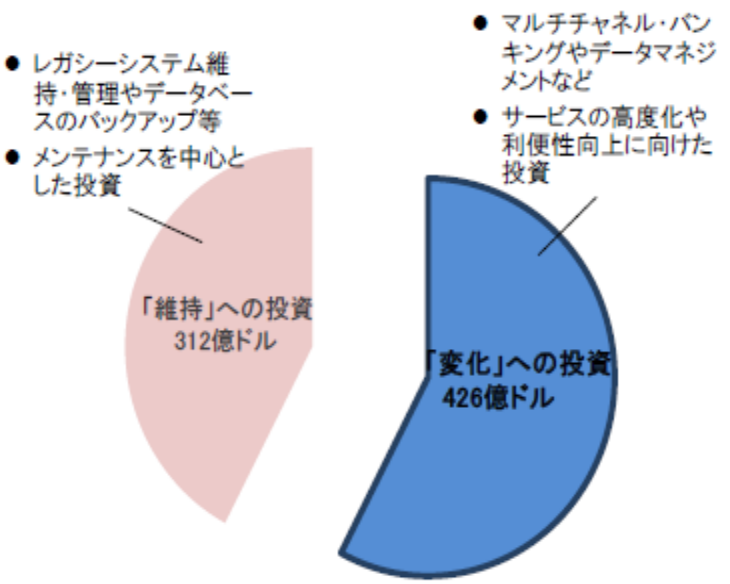
米国の銀行の金融ITは、システム間の連動が少ない**疎結合**であり、システムの一部の変更が全体に影響しないので、変化への対応が比較的柔軟に可能であったと考えられている。

（出典）経済産業省FinTech研究会配布資料（富士通総研 長堀泉氏作成）

金融審議会「決済業務等の高度化に関するスタディ・グループ」での議論を通じて把握された問題意識

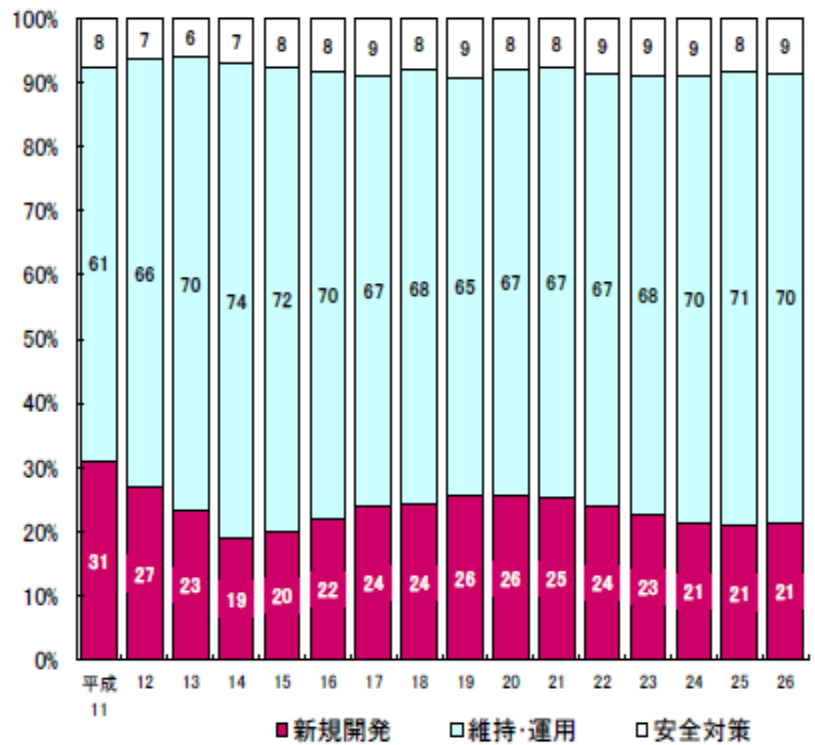
○ 金融審議会では、決済業務の高度化についての審議が進められているが、そこでの議論等を通じ、この問題が、金融グループのIT戦略、更には、グループ全体の経営戦略の問題と密接不可分である、との認識。

米銀のＩＴ予算の優先投資分野（2014年）



（資料）Technology Business Research
（注）総資産額10億ドル以上の北米地域の大手金融機関とITベンダの幹部ら約200人を対象に実施
（出典）決済業務等の高度化に関するスタディ・グループ第2回株式会社日本総合研究所 説明資料

邦銀のシステム関連経費の目的別内訳



（出所）FISC「金融機関業務のシステム化に関するアンケート調査」（平成26年3月）

（出典）金融審議会「金融グループを巡る制度のあり方に関するワーキング・グループ」資料

何が必要なことかが徐々に明確に

伝統的金融機関もFinTech企業との連携を通じて技術進歩の成果を取り入れ、顧客視点からサービスを高度化していくことが可能になる。

オープンネットワークでの利用を前提とした新しい技術

・オープンAPI
・サイバーセキュリティ
・セキュリティデバイス
・生体認証技術
・ブロックチェーン
・AI

金融サービスの高度化

・PFM
・国際送金
・会計サポート
・決済高度化
・新しい融資手法

◆顧客視点
◆UI/UXの改善
◆新しい収益機会

日米の主要FinTech企業の業務領域の違い

サービス分野		業務内容	米国の主なフィンテック企業	日本の主なフィンテック企業
伝統的な銀行と競合する領域	融資	・Web上で貸し手と借り手を募り、信用格付け等を実施して、貸付をマッチングするサービス。P2Pレンディング、ソーシャルレンディングとも呼ばれる。	LendingClub, Prosper, Kabbage,	Maneo,
	決済	・スマートフォン等を利用して個人間送金やクレジットカード決済を行うサービス。伝統的に多くのフィンテック企業が参入してきた。	PayPal, Stripe, Square	LINE Pay,
伝統的な銀行と連携していく領域	PFM	・本人の許諾のもとで多くの銀行の口座情報を集約し、顧客の資産を分かりやすく管理するサービス。	MX, Mint	ﾏﾈｰﾌｫﾜｰﾄﾞ, Zaim, ﾏﾈｰﾂﾘｰ
	会計サポート	・小規模企業向けに、売掛金・買掛金・固定資産等の管理、請求書作成、給与・税金支払いといった経理、税務等のサポートを行うサービス。	Xero, ZenPayroll, Zenefits	ﾏﾈｰﾌｫﾜｰﾄﾞ, freee, ﾒﾘｰﾋﾞｽﾞ
	ロボアドバイザ	・個人の証券投資等への助言やポートフォリオの組成をソフトウエアで行うことにより、安価に提供するサービス。	Motif Investing, Wealthfront, Betterment	お金のﾃﾞｻﾞｲﾝ, ZUU, Finatext

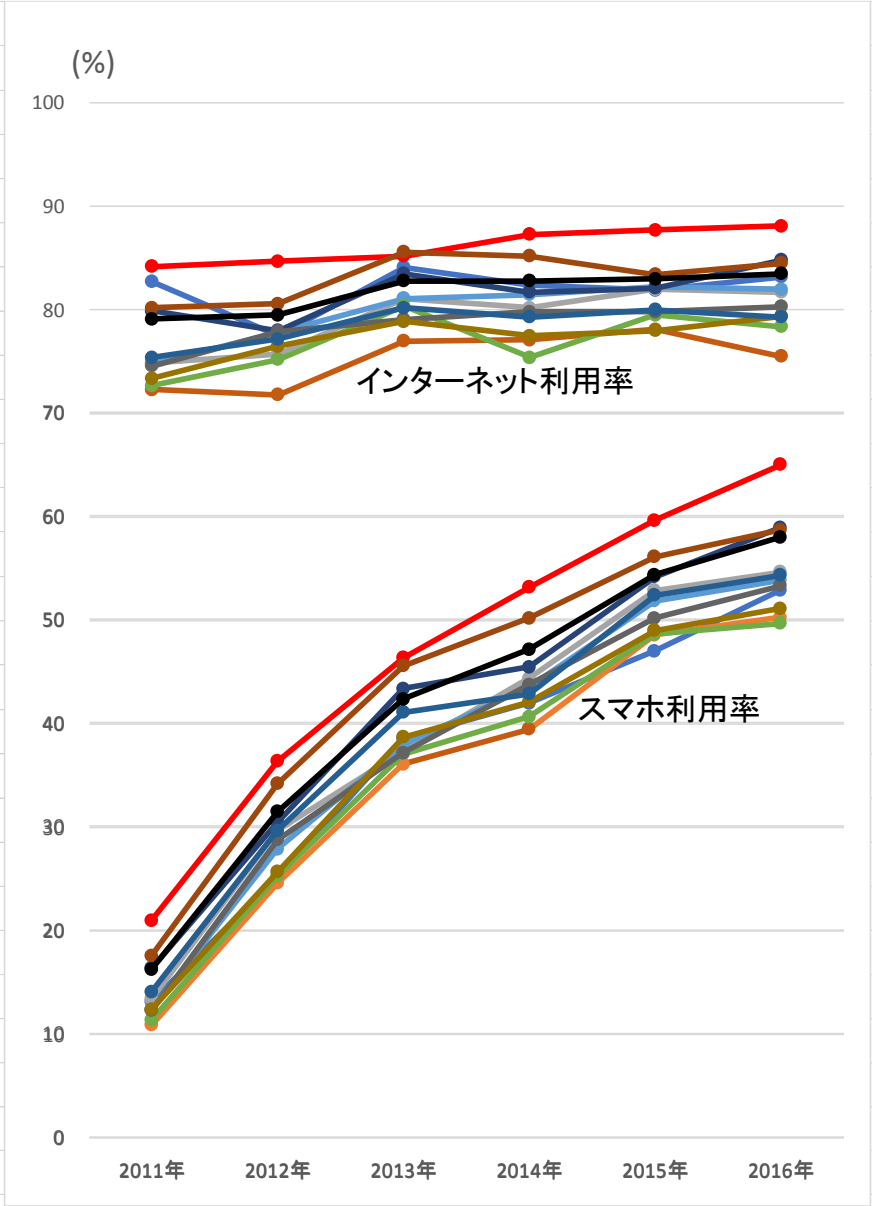
3. インターネットバンキング
～FinTechの前提条件

銀行口座の業態別ネット化比率

業態	インターネット・バンキング契約口座数 (a)	キャッシュカード発行枚数 (b)	銀行口座の推定ネット化比率（a/b）
都銀	3,255 万口座	10,288 万枚	31.6 %
地銀	955	10,687	8.9
第二地銀	107	2,953	3.6
信金	97	5,230	1.9
その他とも計	6,065	33,525	18.1

（出所）金融情報システムセンター(FISC)「金融情報システム白書」2016

地域間のIT格差は大きくない

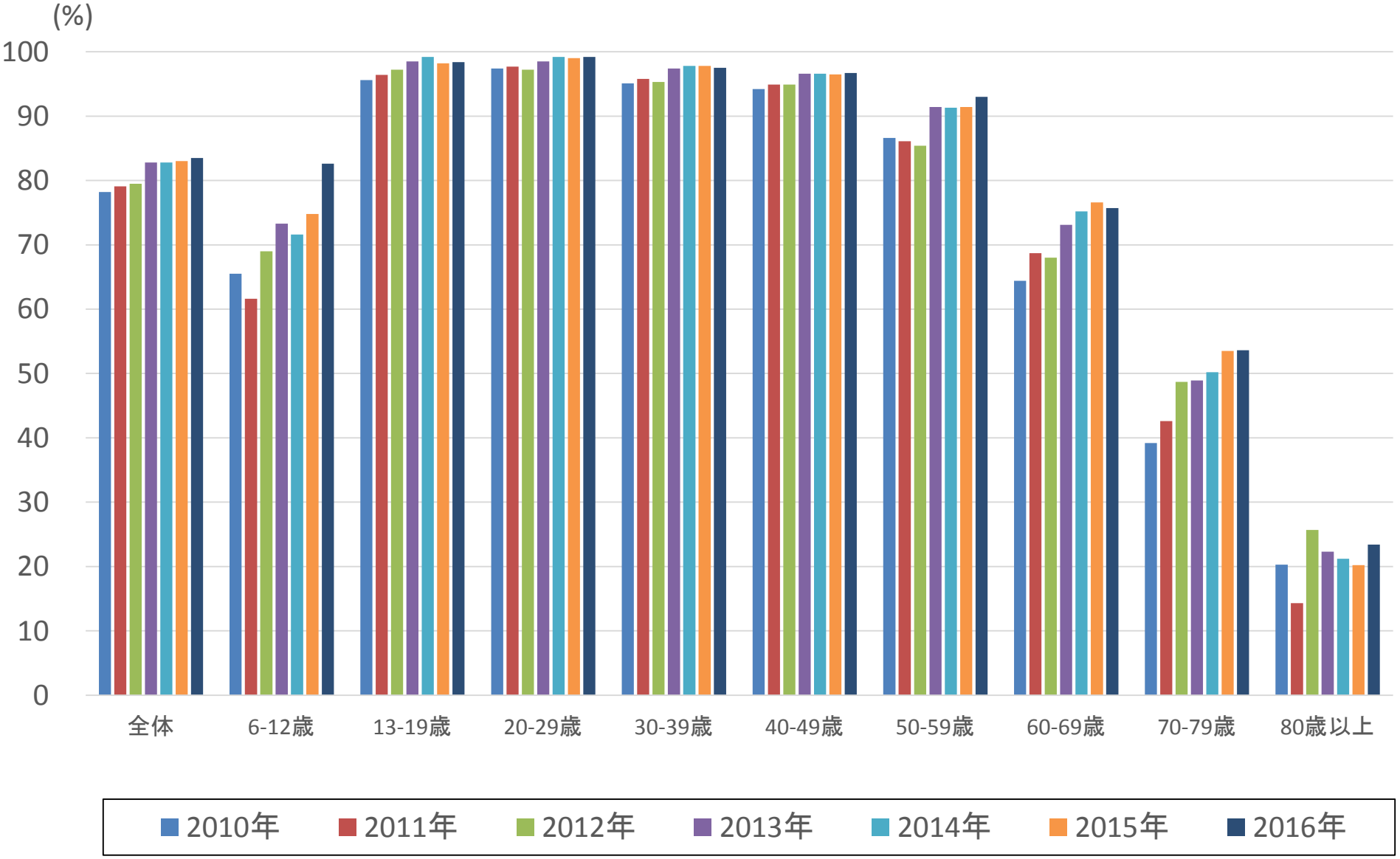


ｲﾝﾀｰﾈｯﾄ利用率	2011年	2012年	2013年	2014年	2015年	2016年
北海道	82.7	77.5	84.1	82.4	81.9	83.2
東北	72.3	71.8	77.0	77.1	78.1	75.5
北関東	74.9	75.7	81.1	80.2	82.0	81.7
南関東	84.2	84.7	85.2	87.3	87.7	88.1
北陸	74.8	77.8	81.1	81.5	82.2	82
甲信越	72.7	75.2	80.4	75.4	79.5	78.4
東海	79.9	78.0	83.5	81.7	82.1	84.8
近畿	80.2	80.6	85.6	85.2	83.4	84.5
中国	74.6	77.9	79.1	79.8	79.8	80.3
四国	73.4	76.5	78.9	77.5	78.0	79.4
九州・沖縄	75.4	77.2	80.2	79.3	80.0	79.3
全国	**79.1**	**79.5**	**82.8**	**82.8**	**83.0**	**83.5**

スマホ利用率	2011年	2012年	2013年	2014年	2015年	2016年
北海道	13.1	25.0	38.5	41.9	46.9	52.8
東北	10.8	24.5	36.0	39.4	48.5	50.2
北関東	13.3	29.6	37.3	44.3	52.8	54.6
南関東	20.9	36.3	46.3	53.1	59.5	64.9
北陸	12.3	27.8	37.9	43.5	51.8	53.8
甲信越	11.3	25.2	37.0	40.6	48.6	49.6
東海	16.3	30.4	43.3	45.4	54.1	58.9
近畿	17.5	34.1	45.5	50.1	56.0	58.6
中国	12.2	28.7	37.1	43.7	50.1	53.2
四国	12.3	25.6	38.6	42.0	48.9	51.1
九州・沖縄	14.0	29.6	41.0	42.8	52.3	54.2
全国	**16.2**	**31.4**	**42.3**	**47.1**	**54.3**	**57.9**

（出典）総務省 「通信利用動向調査」

年齢階層別インターネットの利用状況の推移



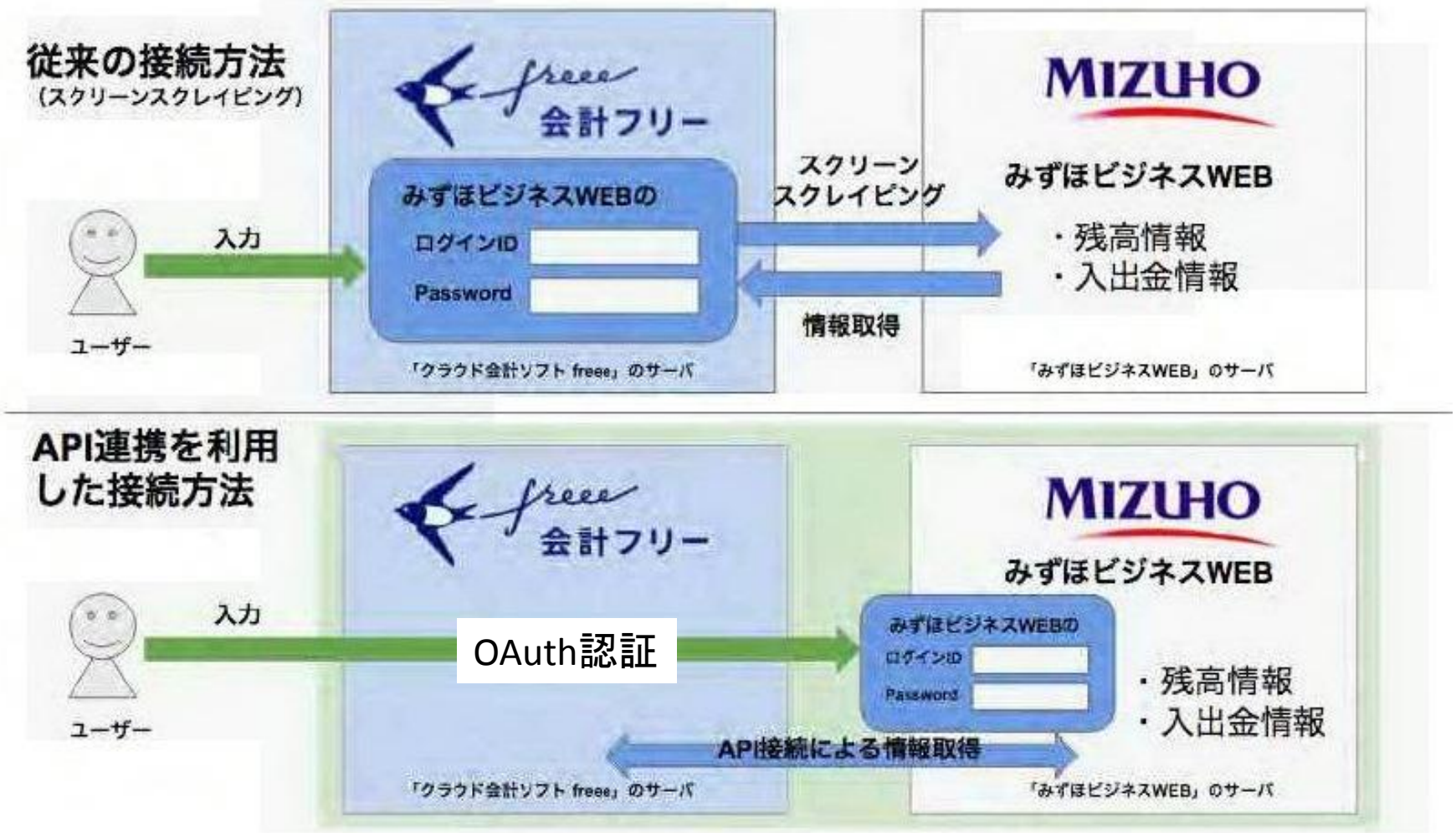
（出典）総務省「通信利用動向調査」

４．金融オープンAPI
～イノベーションの次のハードル

メガバンク、ネットバンクとFinTech企業のAPI接続が始まる

「みずほビジネスWEB」と公式API連携

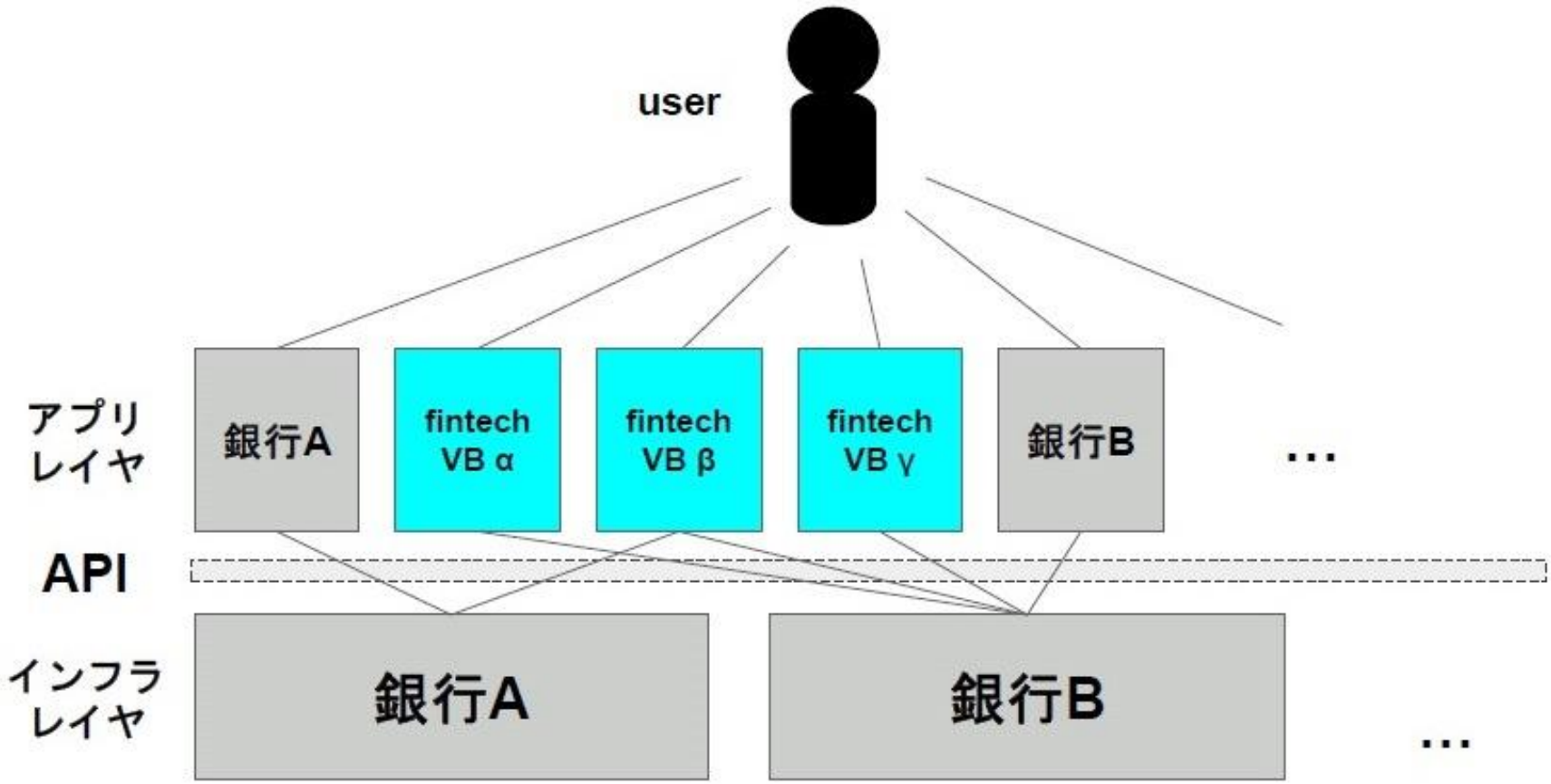
- 国内初のメガバンクとの連携でユーザー利便性向上を目指す



（出典）日本銀行FinTechフォーラム配布資料（freee株式会社 木村康宏氏）

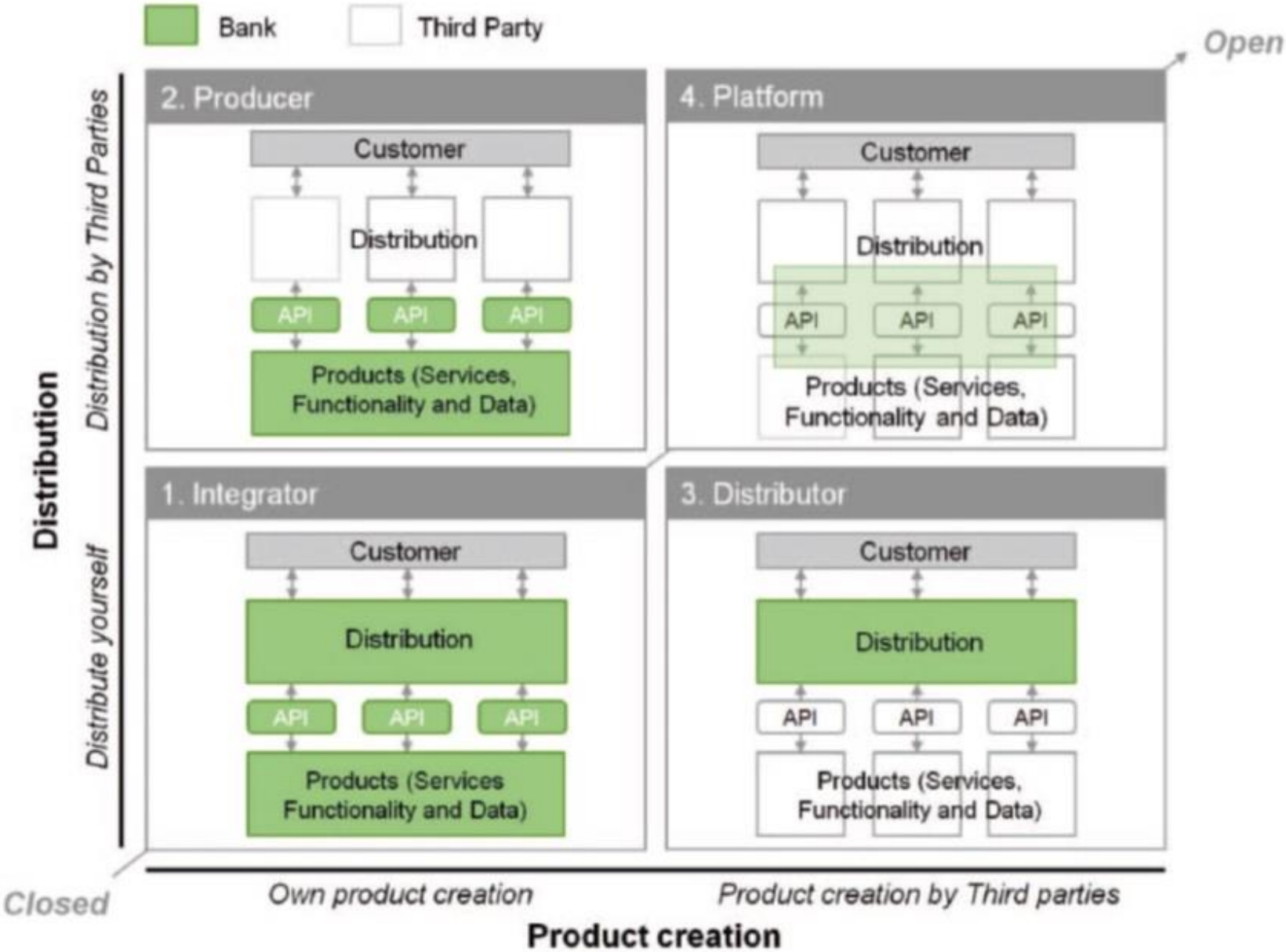
利用者、FinTech企業、銀行の連携の基盤としてのAPI

- 様々なサードパーティのアプリケーションが提供され、金融インフラへのアクセスが多様化することが、ユーザの便益
- 銀行にとっては、オープンイノベーションによって、新サービスをスピーディに立ち上げるための基盤となる



（出典）日本銀行FinTechフォーラム配布資料（freee株式会社 木村康宏氏）

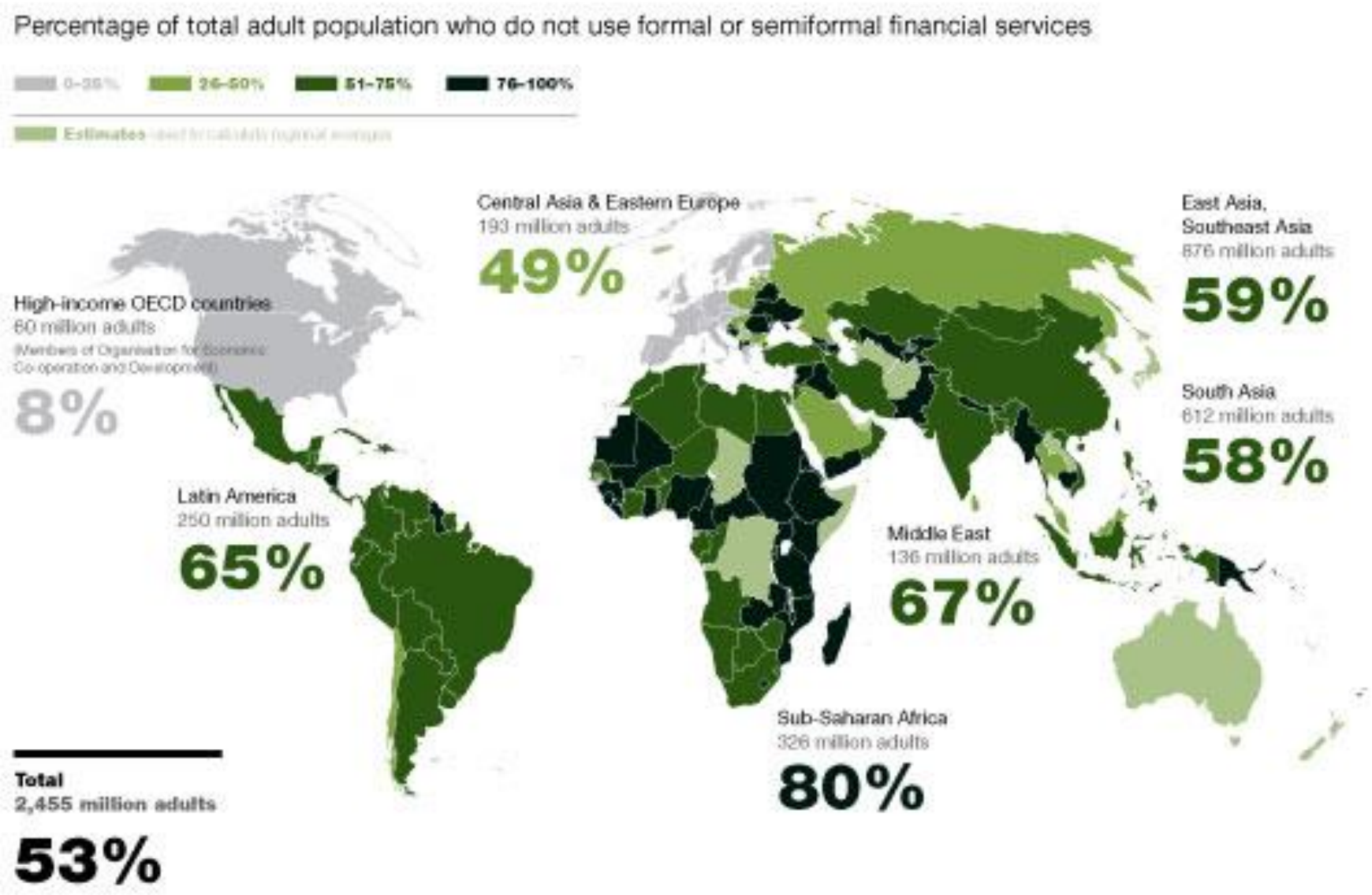
金融サービスにおける銀行とFinTech企業の棲み分け



(Source) "Understanding the business relevance of Open APIs and Open Banking for banks", Euro Banking Association (EBA) Working Group on Electronic Alternative Payments, May 2016

５．新興国におけるキャッシュレス化進展の影響

2010年、世界人口の約半分は銀行が使えなかった



Alberto Chaia, Tony Goland, and Robert Schiff, "Counting the world's unbanked", McKinsey Quarterly, March 2010.

ケニア発のM-PESAが金融包摂を実現

M-PESA: ケニア版電子マネー

携帯電話のSMS機能を使うことで、決済、送金、出金等、様々な使途で使われている。

M-PESで、銀行の支店がなく、現金を持ち歩くことも危険なケニアの地方でも、送金や貯金が可能になった。

図表 4: 国内送金に使用するチャネルの利用率（2006 年・2009 年・2013 年の比較、%）

	2006	2009	2013
家族・友人	57.2	35.7	32.7
バス・マタトゥ（小型乗合バス）	26.7	4.0	5.4
送金サービス	5.3	0.4	1.9
小切手	3.8	1.2	1.3
銀行口座へ直接	9.6	3.2	4.3
郵便局	24.2	3.4	1.3
モバイルマネー	0.0	60.0	91.5

出所：FinAccess National Survey2013（2 つ以上選択可能なため、合計は 100 にならない）

（出所）五味佑子、「金融包摂とモバイルマネーサービスを考える」、国際通貨研究所、2015.11.17

中国におけるモバイル決済の急速な普及

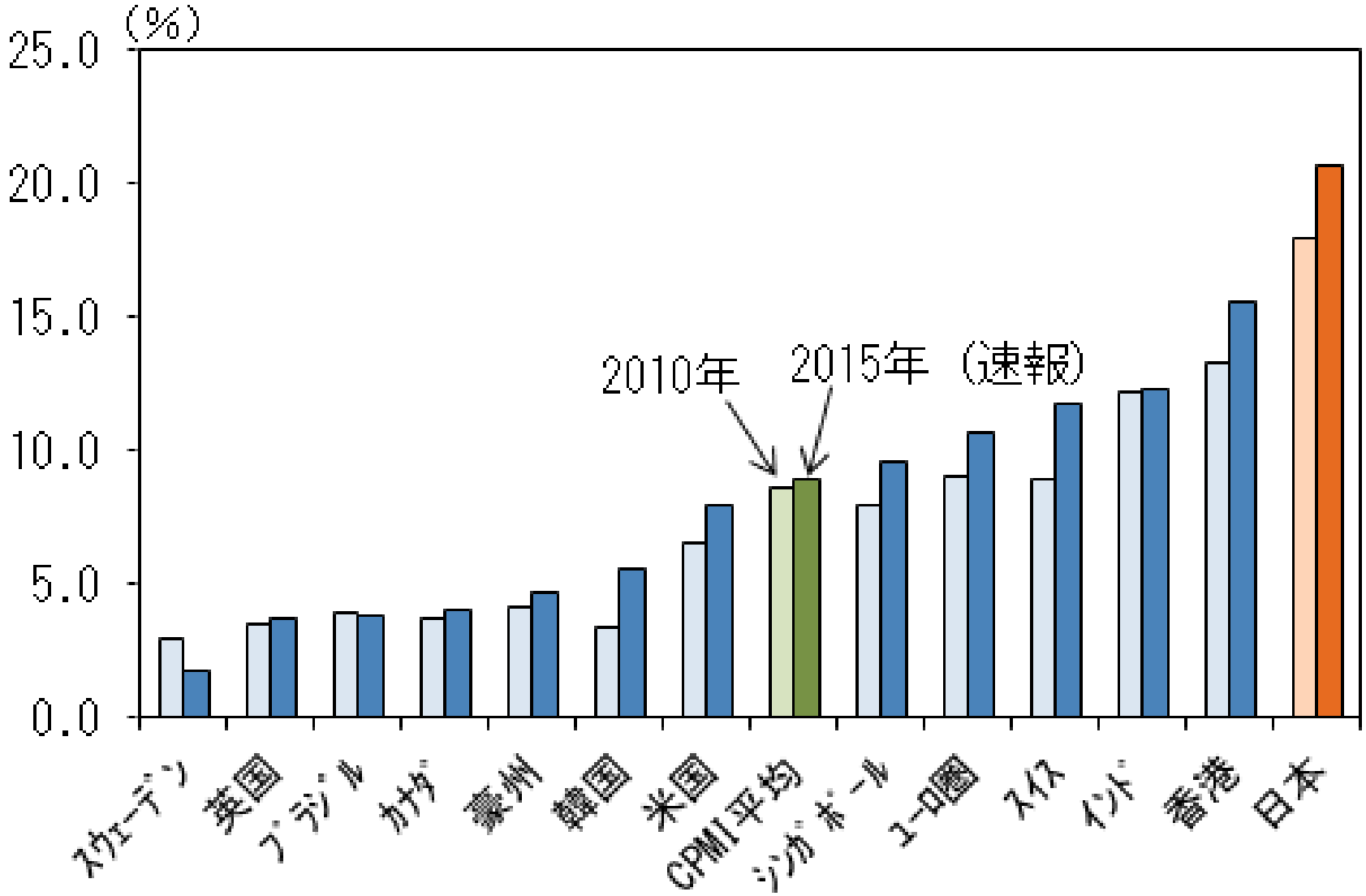
中国・北京の故宮博物院では、紙の入場券が廃止された。

入場者が入口のQRコード看板をスマホで読み取り、モバイル決済で電子入場券を購入する方式に完全移行したのだ。

外国人、老人、何らかの理由でスマホが使えない入場者のために、専用窓口が別途設けられている。

（出典）Twitter @livein_chinaの投稿より

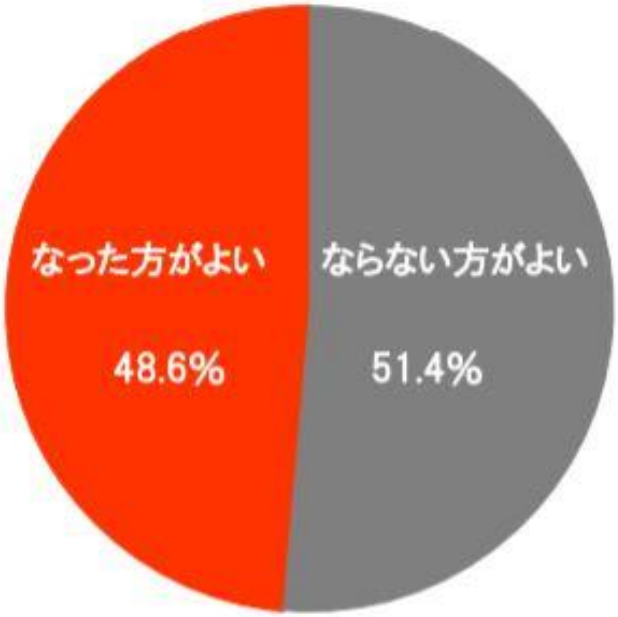
主要国における対GDP通貨流通残高比率の推移（2010→2015年）



（出所）国際決済銀行 決済・市場インフラ委員会

博報堂「お金に関する生活者意識調査」

Q 近い将来、紙幣や硬貨などの現金を使う必要がない「キャッシュレス社会」になるのではないかといわれています。
あなたご自身のお気持ちは「キャッシュレス社会」に「なった方がよい」「ならない方がよい」のどちらに近いですか？（単一回答）



※±10pt以上の差があったもののうち、スコアが高い方に色付け

	調査人数	なった方がよい	ならない方がよい	差
全体	3,600	48.6	51.4	-2.8
男性	1,803	58.7	41.3	17.4
女性	1,797	38.5	61.5	-23.0
男性20代	281	57.7	42.3	15.4
男性30代	340	58.5	41.5	17.0
男性40代	430	58.6	41.4	17.2
男性50代	356	59.0	41.0	18.0
男性60代	396	59.3	40.7	18.6
女性20代	272	36.8	63.2	-26.4
女性30代	333	35.4	64.6	-29.2
女性40代	422	36.7	63.3	-26.6
女性50代	357	42.0	58.0	-16.0
女性60代	413	40.9	59.1	-18.2
	（人）		（%）	（pt）

キャッシュレス化への賛否とその理由

キャッシュレス社会に「賛成」の理由　※自由回答を集計したトップ5、%は賛成した人ベースで算出

賛成の理由		全体	男性	女性	男-女	理由の具体例
1位	現金を持たなくてよいから	14.7	14.9	14.3	0.6	・現金を持ちたくない。不潔だし、財布も重くなる(女性53歳・東京都) ・現金の出し入れで次の方を待たせる場合も多いので、持ち歩かない方が便利(女性63歳・茨城県)
2位	利便性が高いから	10.7	12.2	8.7	3.5	・口座から現金をおろしたり、送金に手間がかかるより、利便性が上がりそう(男性54歳・東京都) ・キャッシュレスは便利。でも、お金を手にしないのは少し淋しい気もする(女性54歳・青森県)
3位	お得だから	6.9	5.5	8.7	-3.2	・クレジットは使うだけでポイントが貯まるし、現金のように手数料を取られず、お得(女性38歳・長野県) ・ポイントが溜まり、銀行の利息よりよい(男性45歳・和歌山県)
4位	やりとりがスムーズだから	6.3	5.5	7.3	-1.8	・通販もクレジットカードがあれば、振込や代引の手間もなくなる(女性30歳・愛知県) ・レジの待ちの時間が減りそう(男性64歳・熊本県)
5位	管理しやすいから	5.5	4.6	6.7	-2.1	・いつ何にお金を使ったかが、インターネットやアプリで管理できれば楽だから(男性39歳・宮城県) ・使用履歴が電子化され、閲覧や見直しができる(女性51歳・大阪府)

キャッシュレス社会に「反対」の理由　※自由回答を集計したトップ5、%は反対した人ベースで算出

反対の理由		全体	男性	女性	男-女	理由の具体例
1位	浪費しそうだから	10.9	7.9	13.3	-5.4	・使った感覚がない売買は湯水の如く金を使いそうで怖い(女性35歳・埼玉県) ・支払いの実感がなくなると、ためらいなく借金や浪費をする人が増えそう(男性26歳・京都府)
2位	お金の感覚が麻痺しそうだから	10.1	5.4	13.8	-8.4	・考えなしに買ってしまいそう。現金は減るのを実感でき、考えて買い物ができる(女性60歳・静岡県) ・いくら使ったかがわかりづらい。支払い可能限度から逸脱する可能性がある(男性34歳・東京都)
3位	お金のありがたみがなくなりそうだから	7.9	5.7	9.6	-3.9	・お金を稼ぐありがたみがわからなくなりそう(女性36歳・宮城県) ・お金の価値が軽いものに変わってきてしまいそう(男性37歳・香川県)
4位	現金は必要だから	6.0	8.6	3.9	4.7	・システムがダウンして混乱を招く事態になった時、やはり現金はあった方がよい(女性52歳・東京都) ・電脳世界の通貨は何らかの障害や天災が発生した際、使い物にならない(男性42歳・大阪府)
5位	犯罪が多発しそうだから	5.7	9.5	2.7	6.8	・暗証番号や個人情報が流出して、犯罪が起きる可能性がある(男性27歳・東京都) ・システムの脆弱性などで不正が行われる心配もある(女性66歳・東京都)

(%)　(pt)

【仮想通貨編】

６．仮想通貨の暴騰と最近の乱高下

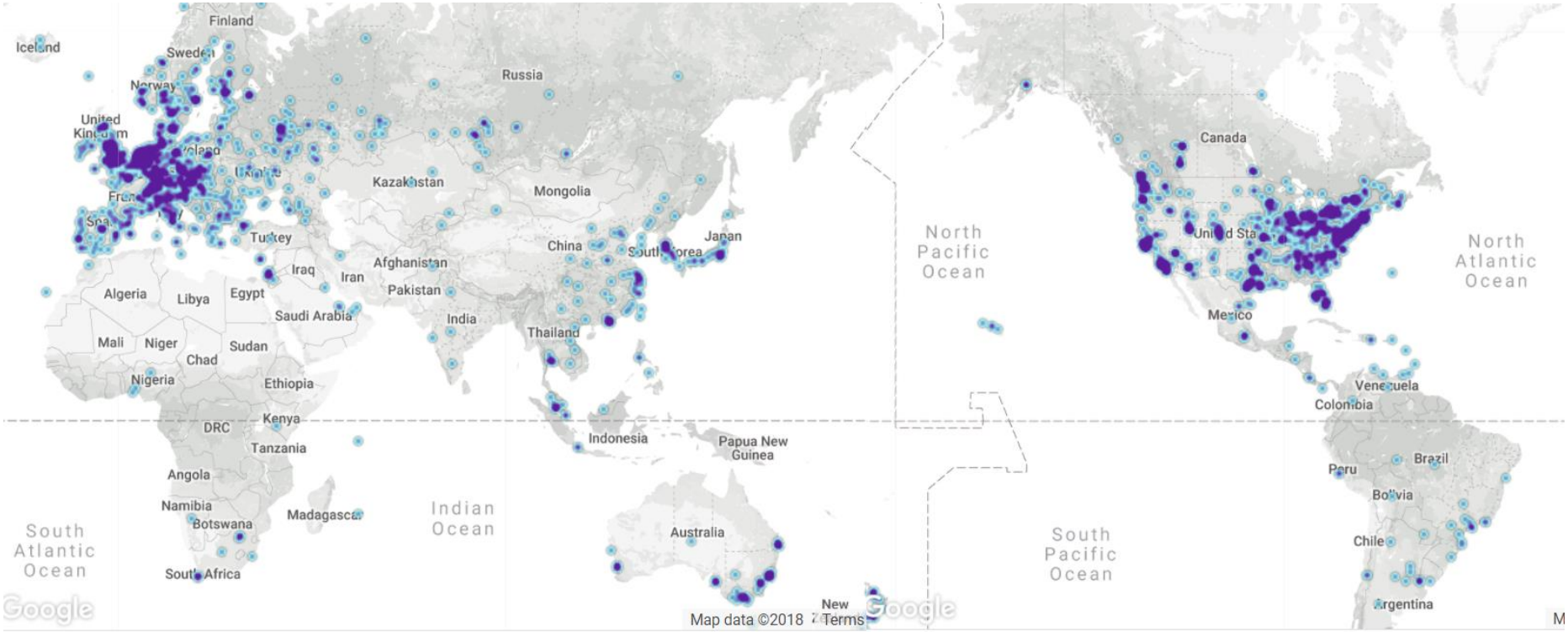
世界のビットコイン・ノードの分布

12109 NODES

24-hour charts »

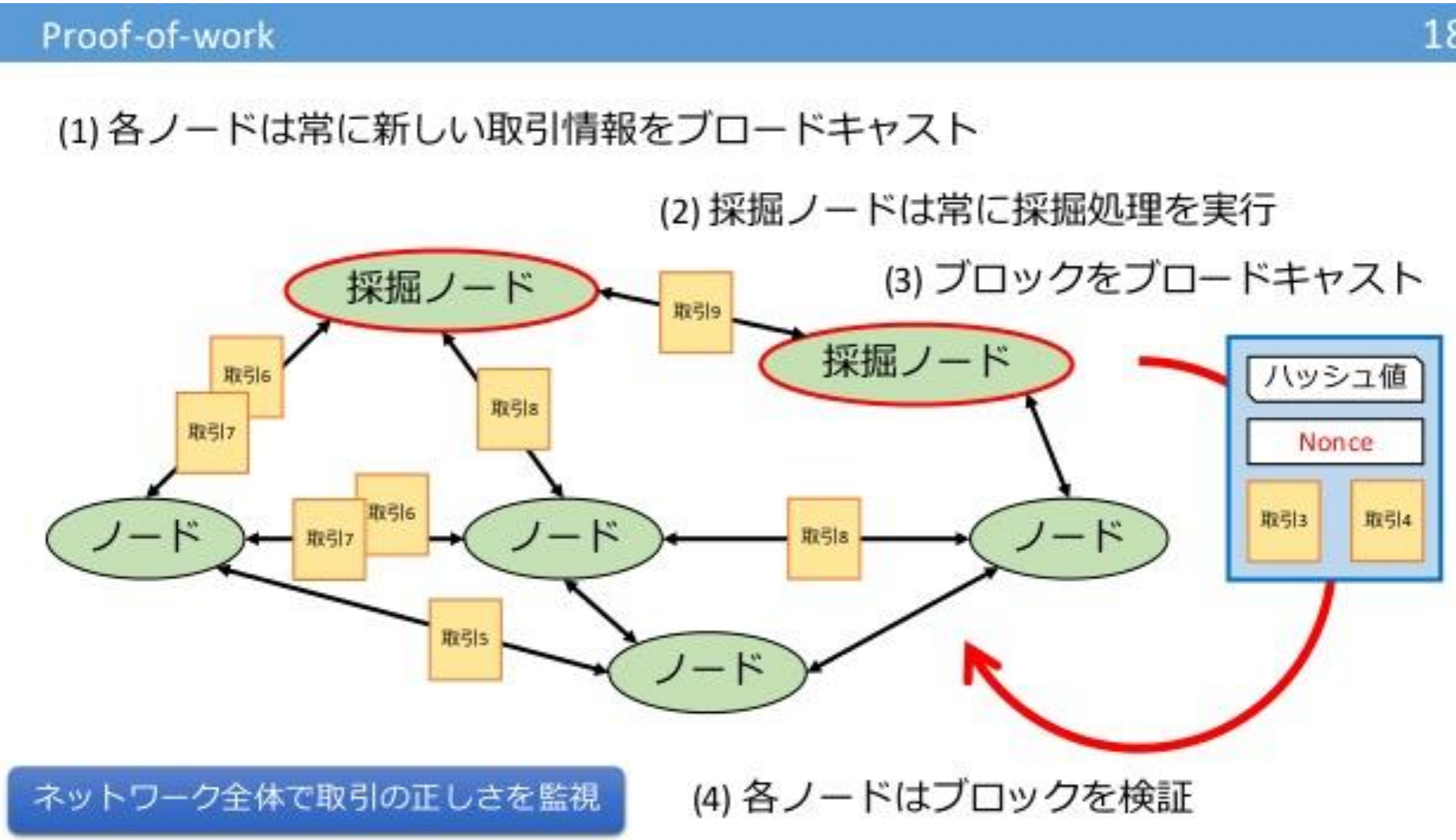
Top 10 countries with their respective number of reachable nodes are as follow.

1. United States (2691)
2. China (2047)
3. Germany (1949)
4. France (697)
5. Netherlands (515)
6. United Kingdom (421)
7. Canada (390)
8. Russian Federation (380)
9. n/a (315)
10. Singapore (227)
11. Japan (212)
12. Hong Kong (183)



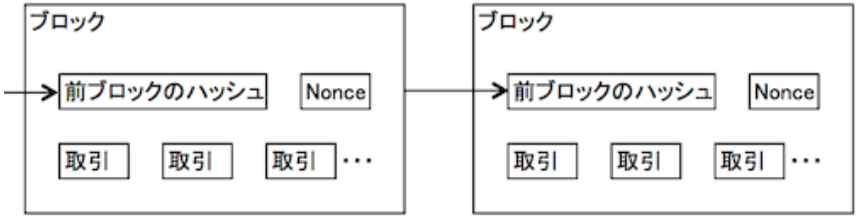
（source）bitnodes.earn.com/

ビットコイン・ノードの役割



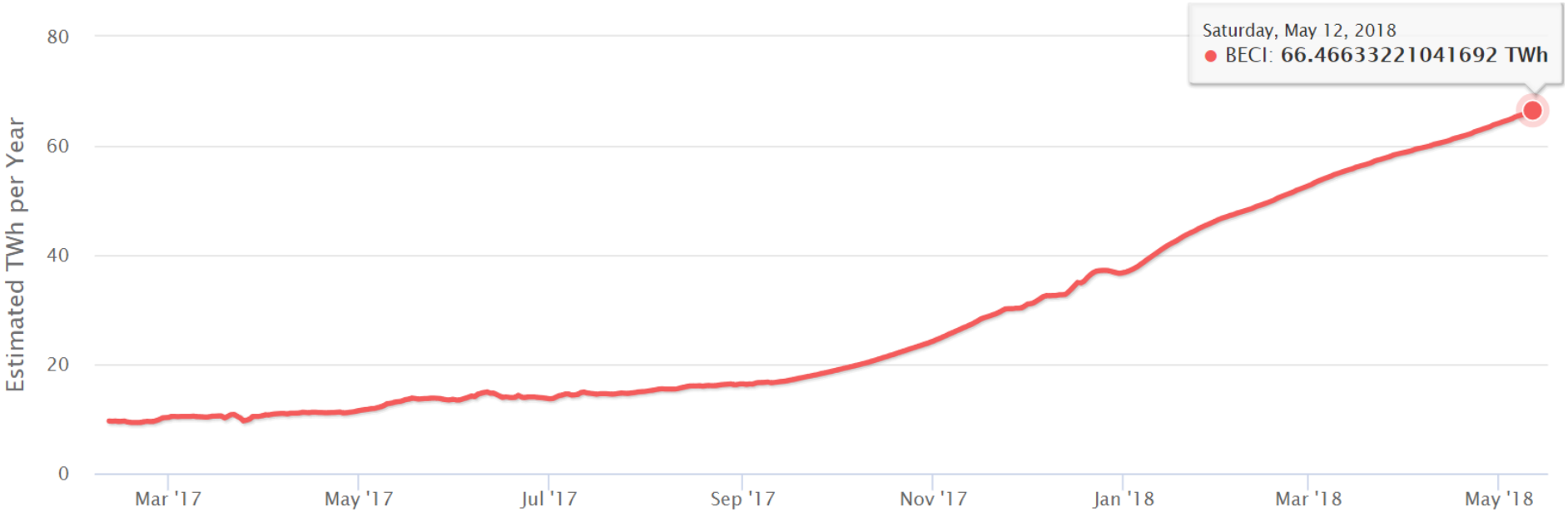
鷲見 拓哉「Bitcoinについて」 https://www.slideshare.net/takuya_sumi/bitcoin-v5

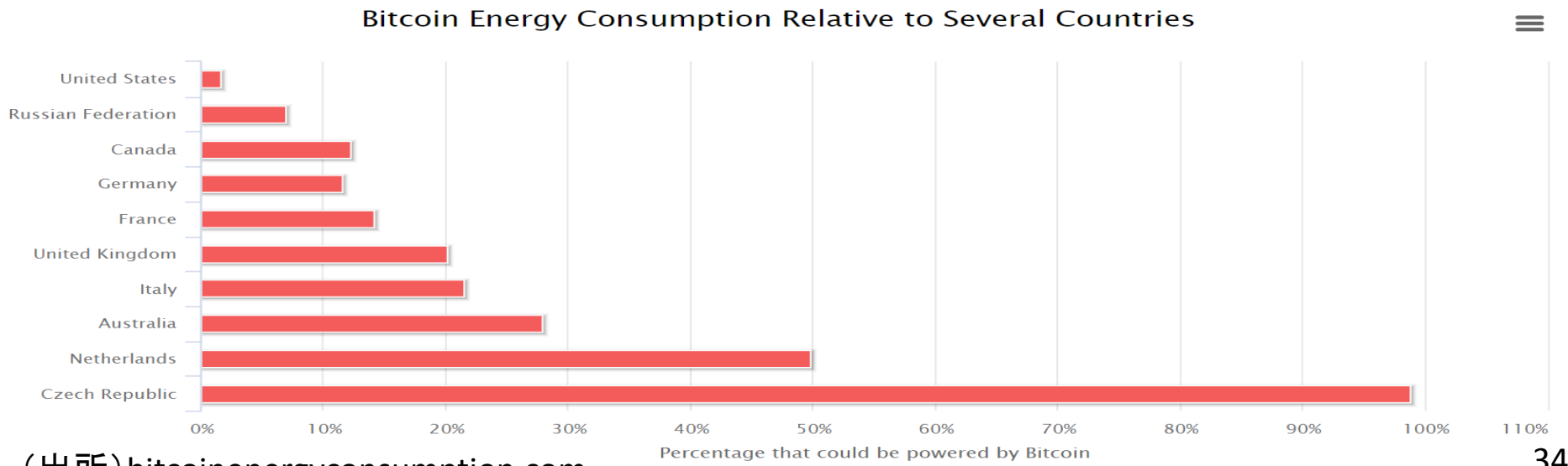
マイニング（採掘）の実態



（出典）https://www.genesis-mining.com/

ビットコインのマイニングが起こす地球環境問題





（出所）bitcoinenergyconsumption.com

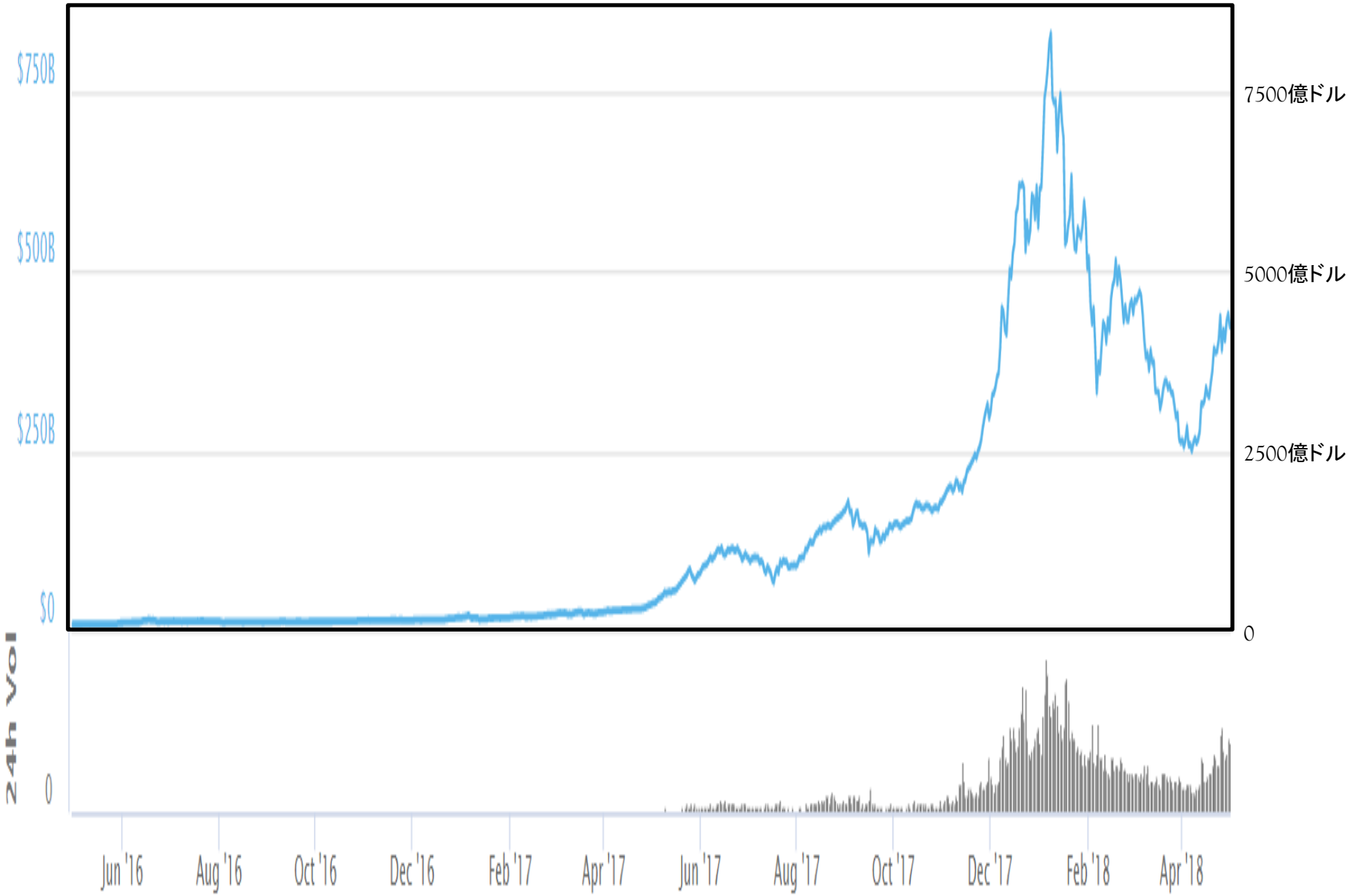
ビットコインの価格と利用者数の推移（2013-16年）

（出所）blockchain.info

ビットコインの価格の推移（直近2年間）

（出所）coinmarketcap.com

全仮想通貨の時価総額の推移（直近2年間）

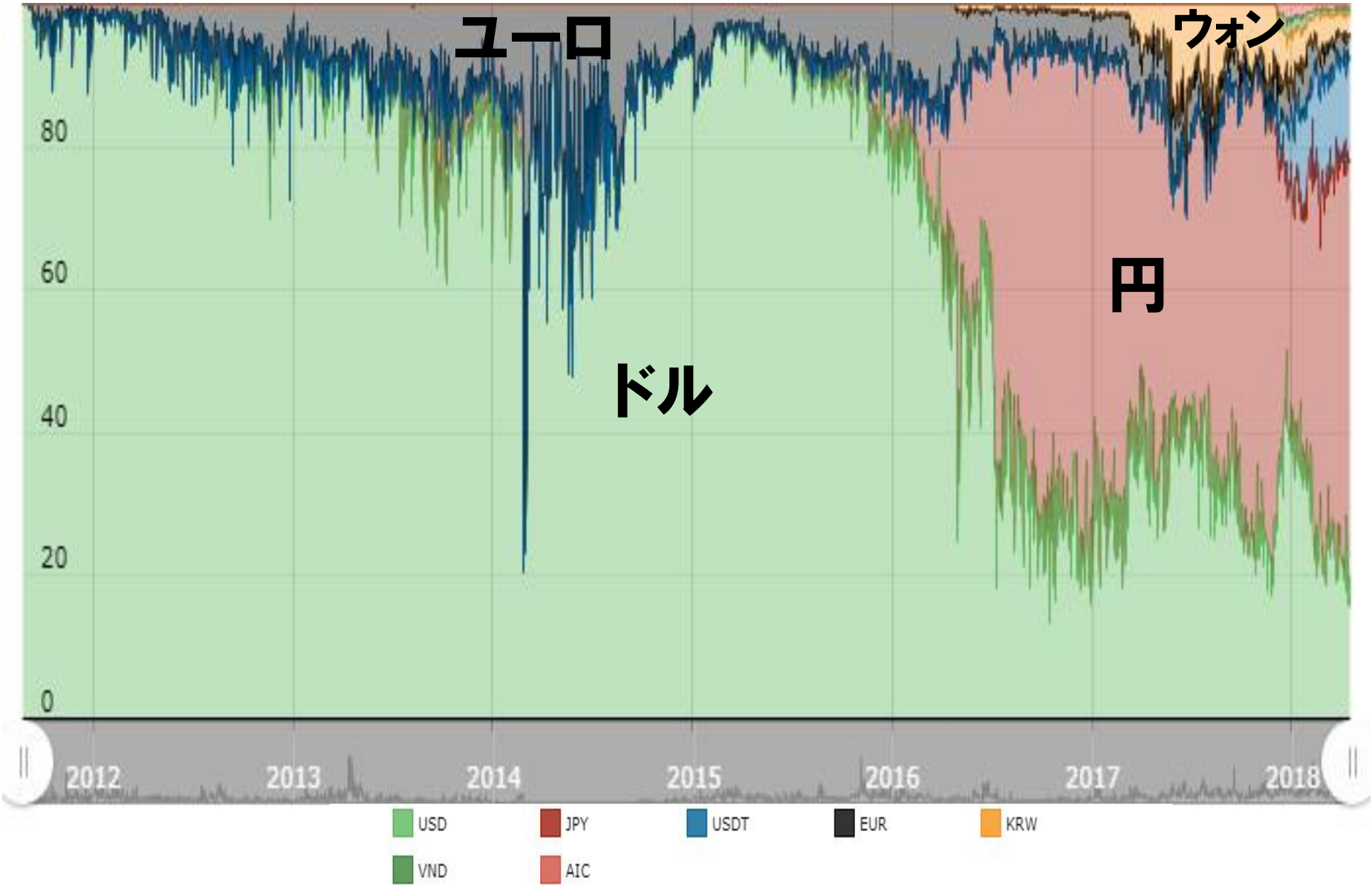


（出所）coinmarketcap.com

仮想通貨の通貨別流通総額の構成比の推移（過去5年間）

（出所）coinmarketcap.com

ビットコインの通貨別取引額の構成比



（出所）www.cryptocompare.com、中国人民元による取引を除くベース

7. ICOの増加と仮想通貨高騰の背景

ICO (Initial Coin Offering) とは

「一般に、ICOとは、企業等が電子的にトークン（証票）を発行して、公衆から資金調達を行う行為の総称です。トークンセールスと呼ばれることもあります。」
（金融庁、「ICO（Initial Coin Offering）について～利用者及び事業者に対する注意喚起～」、29.10.27 ）

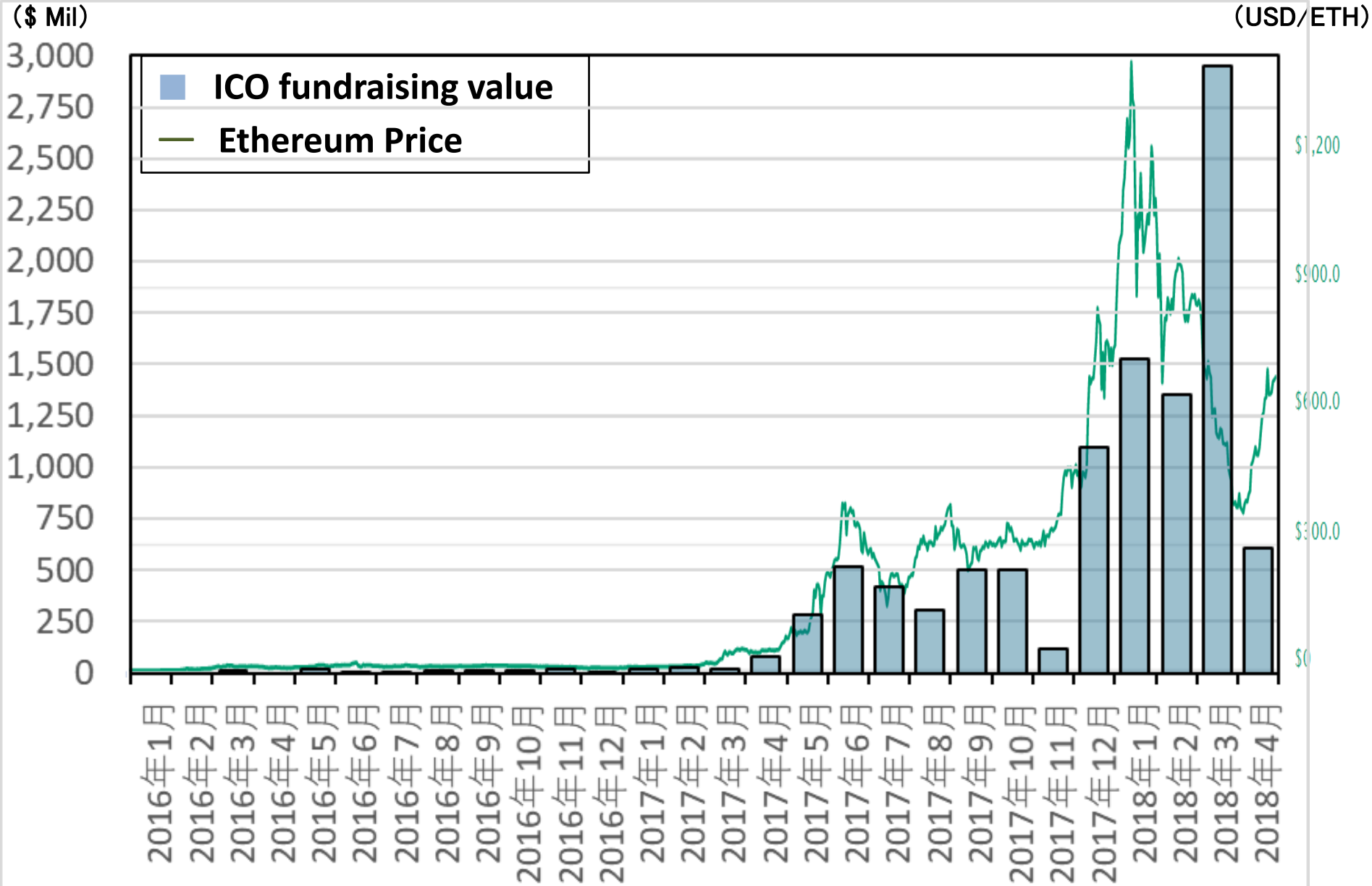
技術的には、イーサリアムのスマートコントラクトを利用したトークンで、ERC-20 Token Standard（EIP20）に準拠したものが用いられることが多い。

EIP: 20（2017-9-11）
Title: ERC-20 Token Standard
Created: 2015-11-19

Simple Summary
A standard interface for tokens.

Abstract
The following standard allows for the implementation of a standard API for tokens within smart contracts. This standard provides basic functionality to transfer tokens, as well as allow tokens to be approved so they can be spent by another on-chain third party.

ICOによる資金調達額とイーサリアム価格の推移



（出典）www.coinschedule.com, www.coingecko.com

発行時期別のICOトークン収益率

2017年ICOが行われたTokenのうち、スキャム（詐欺）を除外し、取引所に上場され、100万ドル以上資金調達に成功したもの（115件）について、発行時期（Q1～Q4）別に、上場初日に売却した場合（Day−1）と調査時点まで保有した場合（Current）の収益率の平均値、中央値を計算したもの。年前半発行のものは大きく値上がりしたが、年後半に発行したものの収益率は必ずしも高いとは言えないレベルであることがわかる。

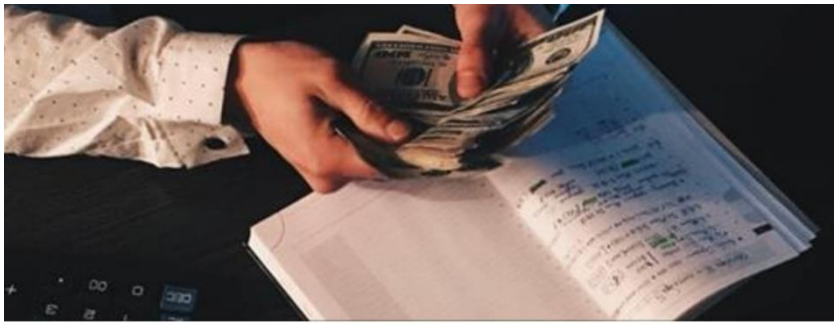
Day One ICO Trading Results

			Day-1 Return		Current Return	
	USD	Nr	Average	Median	Average	Median
Q1 17	$16M	6	5.1x	3.9x	18.3x	13.3x
Q2 17	$892M	43	3.5x	1.9x	3.5x	1.8x
Q3 17	$812M	52	1.6x	1.1x	1.9x	0.8x
Q4 17	$341M	14	1.6x	1.1x	1.3x	1.1x
	$2,061M	**115**	**2.5x**	**1.4x**	**3.2x**	**1.2x**

Source: TokenData.io

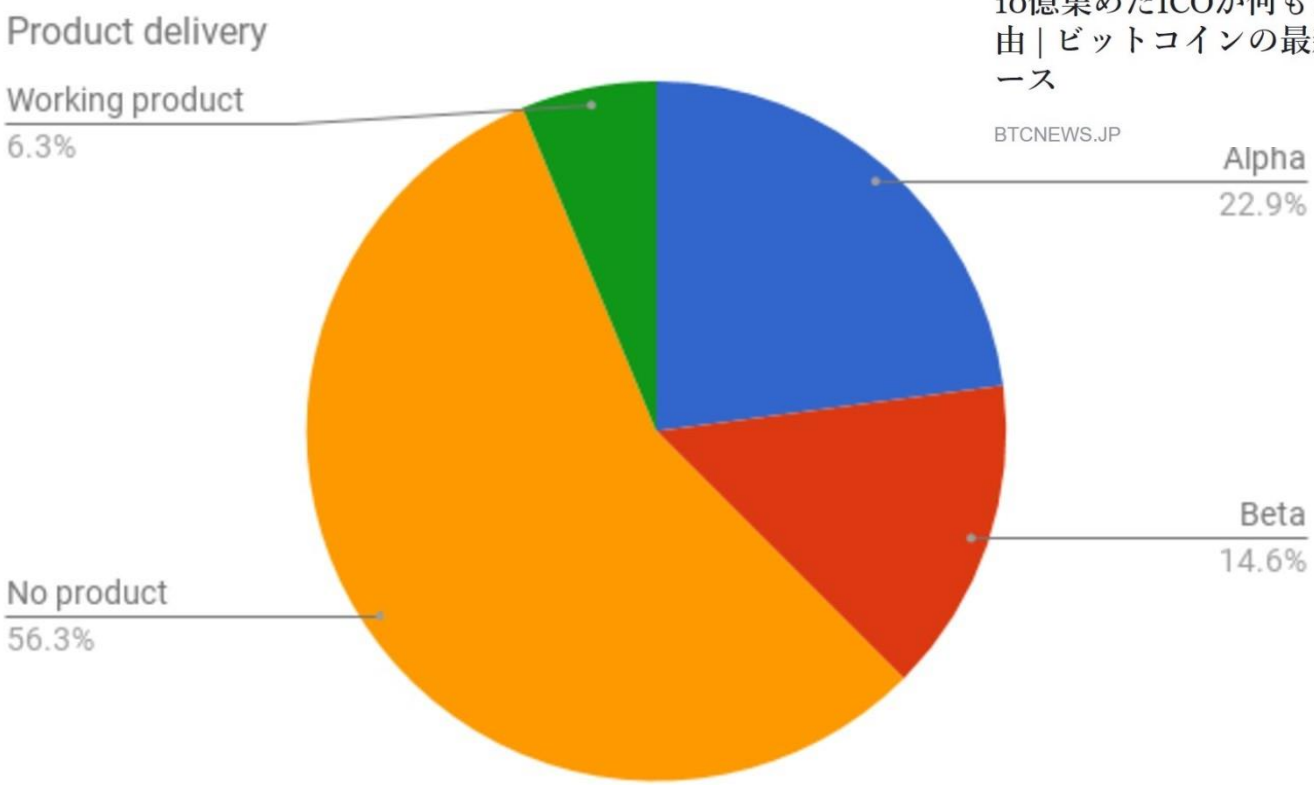
ICOの半数以上(56%)は まだ何かしらのプロダクトすら存在しない

- Working product: **3 (6.25%)**
- Beta product: **7 (14.58%)**
- Alpha product: **11 (22.92%)**
- No product: **27 (56.25%)**



10億集めたICOが何もプロダクトをローンチできない理由 | ビットコインの最新情報 BTCN | ビットコインニュース

BTCNEWS.JP



東 晃慈、「10億集めたICOが何もプロダクトをローンチできない理由」、2017.09.01、https://btcnews.jp/2ojkkse512376/

米国SEC(証券取引委員会)の検討結果の公表

U.S. SECURITIES AND EXCHANGE COMMISSION

Sea
COMP

ABOUT | DIVISIONS | ENFORCEMENT | REGULATION | EDUCATION | FILINGS | NEWS

- Newsroom
- Press Releases
- Public Statements
- Speeches
- Testimony
- Spotlight Topics
- Media Kit
- Press Contacts
- Events
- Webcasts

Press Release

SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities

U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations

FOR IMMEDIATE RELEASE
2017-131

Washington D.C., July 25, 2017— The Securities and Exchange Commission issued an investigative report today cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws. Such offers and sales, conducted by organizations using distributed ledger or blockchain technology, have been referred to, among other things, as "Initial Coin Offerings" or "Token Sales." Whether a particular investment transaction involves the

SECは2016年6月に発行されたthe DAOプロジェクト(後述)で利用されたトークン発行が、米国証券法上の有価証券の募集・売出に該当し得るとの見解を表明。

中国の通貨当局はICOを全面禁止

中国人民银行
THE PEOPLE'S BANK OF CHINA

About PBC | Management Team | Former Governors | News | Speeches | Monetary Policy | Financial Market | Survey & Stat. | Regulations | Financial Stability | Publications | Working Paper | Links |

search Adv.Search

Wed. 13 .9 2017 | You are here: Home > News

Public Notice of the PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on Preventing Risks of Fundraising through Coin Offering

Font Size Big Medium Small 2017年09月08日

print close

Recently, a large number of fundraising activities through issuing tokens including Initial Coin Offering (ICO) have taken place in China, giving rise to speculation and inviting suspicion of illegal financial activities. These activities have disrupted the economic and financial order. To implement the spirit of the National Financial Work Conference, protect the legitimate rights and interests of investors and manage financial risks, and in accordance with Law of the People's Republic of China on the People's Bank of China, Law of the People's Republic of China on Commercial Banks, Law of the People's Republic of China on Securities, Law of the People's Republic of China on Cyber Security, Regulation of the People's Republic of China on Telecommunication, Measures for Banning Illegal Financial Institutions and Illegal Financial Business and Activities, and other laws and regulations, the relevant matters are hereby announced as follows:

I. The Essential Attributes of Fundraising Through Coin Offering

Financing through coin offerings refer to financing bodies raising virtual currencies such as Bitcoin or Ethereum from investors through

日本の金融庁もICOに対する注意喚起を公表

ＩＣＯ（Initial Coin Offering）について
～利用者及び事業者に対する注意喚起～

29.10.27 金融庁

１．ＩＣＯとは

○　一般に、ＩＣＯとは、企業等が電子的にトークン（証票）を発行して、公衆から資金調達を行う行為の総称です。トークンセールと呼ばれることもあります。

２．利用者の方へ（ＩＣＯのリスクについて）

○　ＩＣＯで発行されるトークンを購入することには、次のような高いリスクがあります。

✓ **価格下落の可能性**
トークンは、価格が急落したり、突然無価値になってしまう可能性があります。

✓ **詐欺の可能性**
一般に、ＩＣＯでは、ホワイトペーパー（注）が作成されます。しかし、ホワイトペーパーに掲げたプロジェクトが実施されなかったり、約束されていた商品やサービスが実際には提供されないリスクがあります。また、ＩＣＯに便乗した詐欺の事例も報道されています。

（注）ＩＣＯにより調達した資金の使い道（実施するプロジェクトの内容等）やトークンの販売方法などをまとめた文書をいいます。

○　トークンを購入するに当たっては、このようなリスクがあることや、プロジェクトの内容などをしっかり理解した上で、自己責任で取引を行う必要があります。

南米におけるデジタル法定通貨の実装

先進主要国における慎重な検討に比べ、いち早く、中央銀行がデジタル法定通貨を発行した地域がある。それは、南米である。

エクアドル、ウルグアイ、ベネズエラといった国々では、国が発行するデジタル通貨は、検討課題ではなく、現実である。これは、こうした国々が長い期間、インフレに悩んできたことと関係している。

ベネズエラの奇妙なデジタル法定通貨

2018年1月、ベネズエラのマドゥロ大統領は、同国の生産する石油に裏付けられたデジタル法定通貨「ペトロ（Petro）」の最初の1億ペトロ分の発行を命じた。同大統領によれば、1ペトロは1バーレルのベネゼエラ産石油の価値を持つとされている。マドゥロ大統領は今回、ペトロを支援するため、オリノコ重質油帯のアヤクーチョ油田1を引き当てることを約束した。同大統領はさらに、国内のダイヤモンド鉱床とともにアルコ・ミネロ金鉱も割り当てるという。

ペトロはビットコインと同様のブロックチェーン技術を用いて発行、流通する。その実態はERC-20トークンである。つまり、「国家によるICO」なのだ。

ベネズエラは、長年続いた反米主義のチャベス大統領の没後、マドゥロ大統領が就任したばかりである。米国による経済制裁を受け、経済は疲弊し、実質的なインフレ率は極めて高い水準になっている。そうした数多くの課題を解決する「魔法の杖」として、デジタル法定通貨の構想が実現してしまったことを危惧する報道も多い。

ベネズエラPetroをめぐる争い

2018年1月10日、ベネズエラ議会は、新通貨「Petro」に関する大統領令を違憲と判断した。この決定により、関連する大統領令は失効すると報じられたが、マドゥロ大統領はPetroの発行を決行した。

Venezuela's Oil-Backed Cryptocurrency Declared Illegal - Bitcoin News

The Venezuelan parliament has declared the oil-backed cryptocurrency created by President Nicolas Maduro illegal and in violation of the country's Constitution....

NEWS.BITCOIN.COM

ベネズエラはPetroで50億ドルを調達か

根拠なき高騰の危うさ

は「部分的な債務不履行（デフォルト）」と格付けされ、金融市場で資金を調達することは困難だ。

地元大学の調査では、国民の9割が貧困に陥り、国民の6割は十分に食料が買えず体重が17年の1年間で平均11キロ・グラム減った。

原油の裏付け？

「国債を発行できない国が、なぜ仮想通貨で資金調達できるのか。国債とどこが異なるのか」。金融市場や専門家は一様にペトロに懐疑的な目を向ける。

ペトロについて、政府の発表からは、次のような実態が浮かび上がる。

まず、利子はつかず、満期が来て払い込んだ額が返ってくることもない。国債は利子が受け取れ、満期には発行国が破綻しない限り元本が返ってくる。投資家にはペトロの方が条件は不利だ。ベネズエラ政府は「原油が裏付けだ」としているが、原油との交換は保証していない。

さらに、「通貨」としての機能も不十分だ。

米ブルームバーグ通信などによると、ペトロを購入できるのは当面、ドルやユーロ、ビットコインなどに限られ、現地通貨のボリバルは対象外。他方、ペトロを使えるのは同国内のみだ。購入するのは外国人が中心なのに使えるのは同国内だけという矛盾がある。

そのようなペトロが50億ドルもの資金を集めることができたのは「仮想通貨」だからにほかならない。京都大学の岩下直行教授は、「ベネズエラ政府が海外の投資家向けに債券を発行しても1ドルも手に入らないだろう。ペトロは『国営ICO』だ」と指摘する。

ICOは新興企業が新たに事業を始める際、議決権の付与や配当の支払いなど株式発行のような責任を負わずに資金を手軽に集める手法として、世界中で浸透している。返済や利払いの義務なしで集めた資金を自由に使えるという点で、ペトロはICOと同じだ。

一方、多額の資金を集め

（出典）読売新聞2018年3月16日朝刊

８. コインチェック事件と仮想通貨のセキュリティ

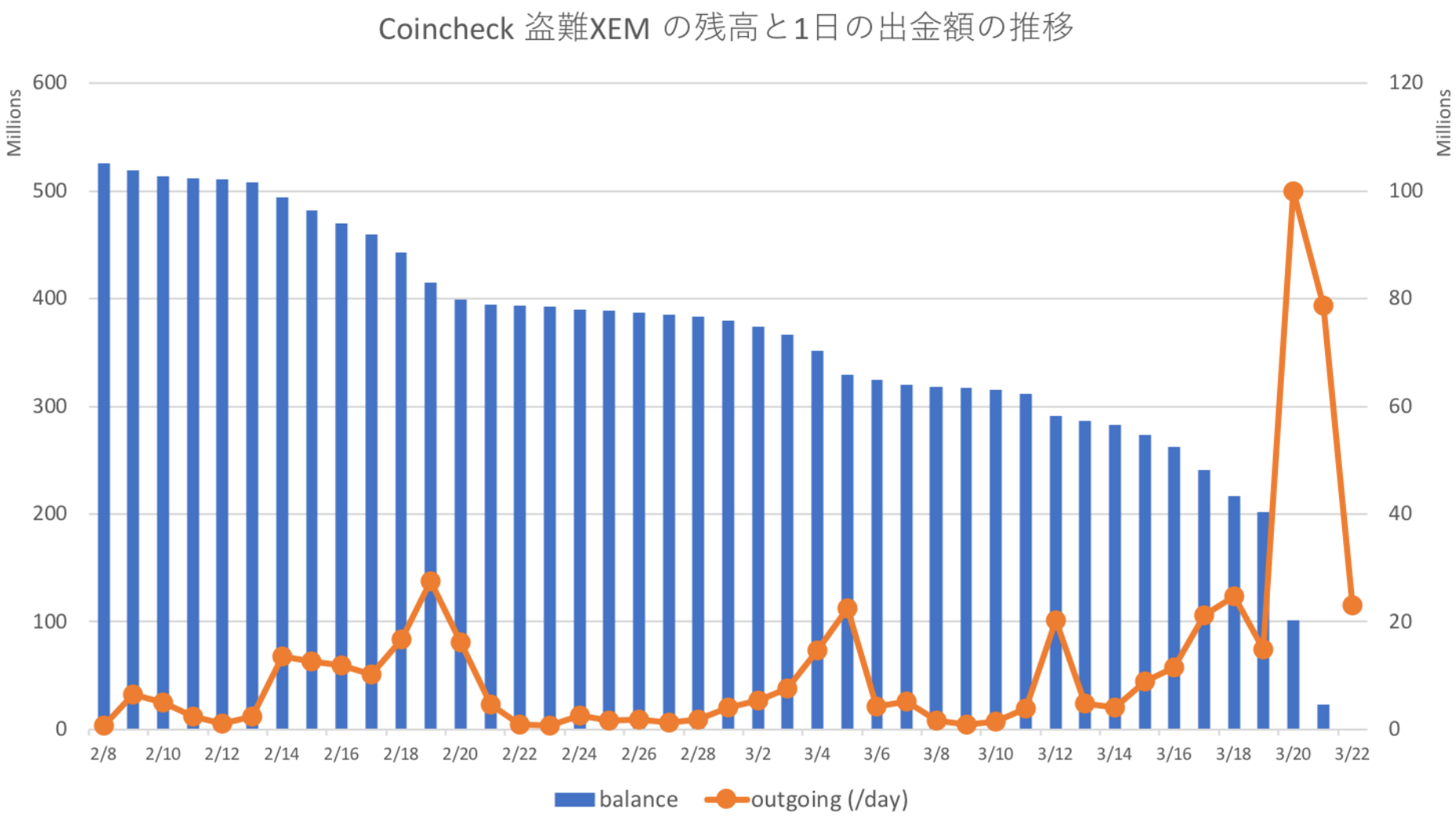
仮想通貨 不正流出事件の概要

- コインチェック社は、顧客から預かった仮想通貨ネム580億円分を、インターネットに接続されたウォレットと呼ばれる装置で管理していた。
- ウォレットには、その情報を書き換えるための秘密鍵と呼ばれる文字列が格納されていて、この秘密鍵を使って取引が行われる。
- 本来、部外者に知られてはならない秘密鍵を攻撃者に勝手に使われて、世界中のコンピュータの情報を書き換える指令が出され、580億円分のネムは、コインチェック社のアドレスから、犯人が用意したアドレスに送金されてしまった。

コインチェック事件におけるNEMの動き

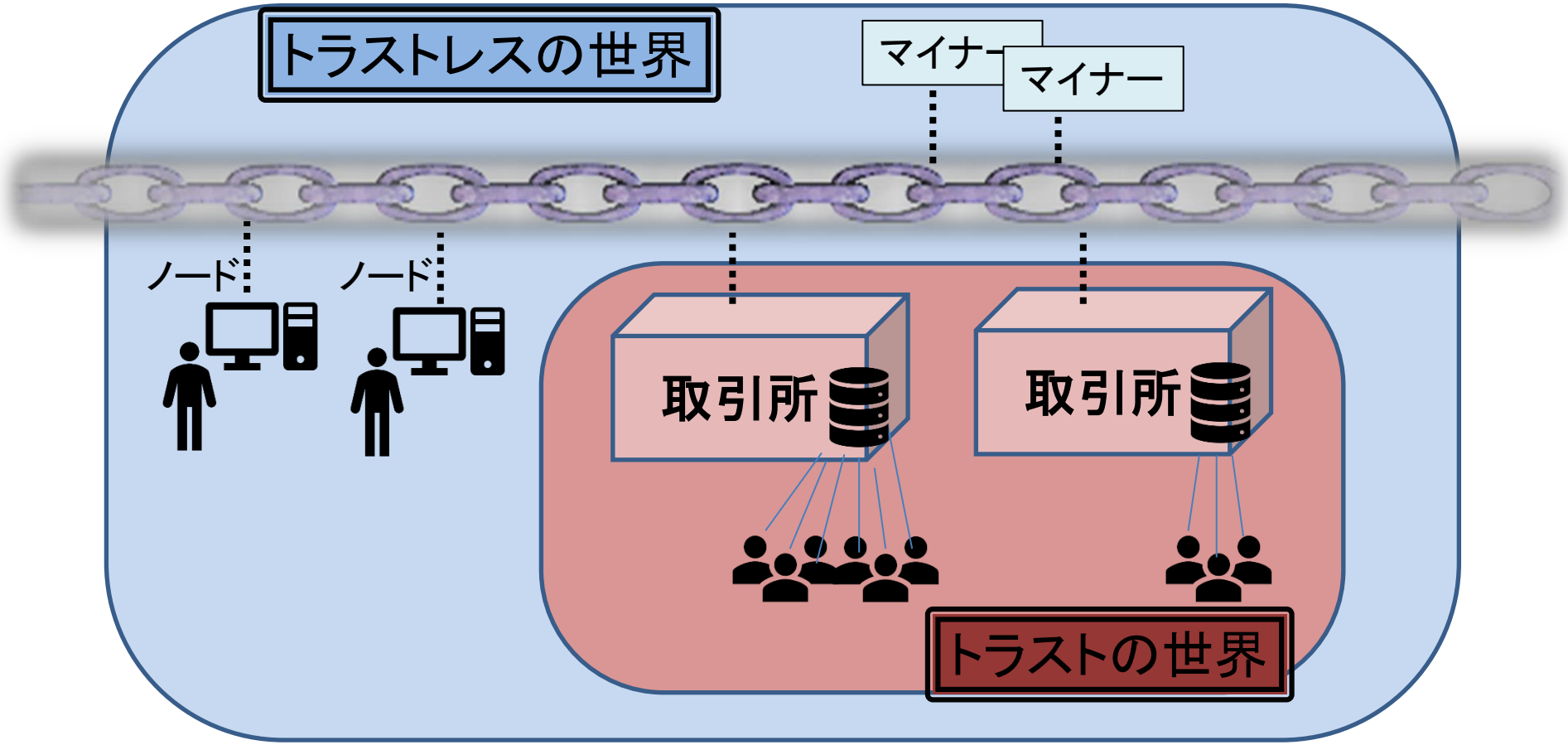
時刻	金額(XEM)	送金元	送金先
2018/1/26 8:26	800,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 4:33	1,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:35	1,500,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 3:29	92,250,000	NC4C6PSUW5	NA6JSWNF24Y
2018/1/26 3:28	100,000,000	NC4C6PSUW5	NDDZVF32WB
2018/1/26 3:18	100,000,000	NC4C6PSUW5	NB4QJJCLTZW
2018/1/26 3:14	100,000,000	NC4C6PSUW5	NDZZJBH6JZP
2018/1/26 3:02	750,000	NC4C6PSUW5	NBKLQYXEIVE
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWEIZ
2018/1/26 2:58	50,000,000	NC4C6PSUW5	NA7SZ75KF6Z
2018/1/26 2:57	30,000,000	NC4C6PSUW5	NCTWFIOOVIT
2018/1/26 0:21	3,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:10	20,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:09	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:08	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:07	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:06	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:04	100,000,000	NC3BI3DNMR2	NC4C6PSUW5
2018/1/26 0:02	10	NC3BI3DNMR2	NC4C6PSUW5

盗まれたNEMはどうなったか？



「トラストレスの中のトラスト」構造の問題

ビットコインの取引のうち、マイニングの対象となるものは、ブロックチェーンの仕組みにより安全性が担保されている。しかし、交換所での取引は交換所限りで処理され、マイニングの対象とならない。取引所経由で間接的に参加している利用者は、トラストの世界に居る。



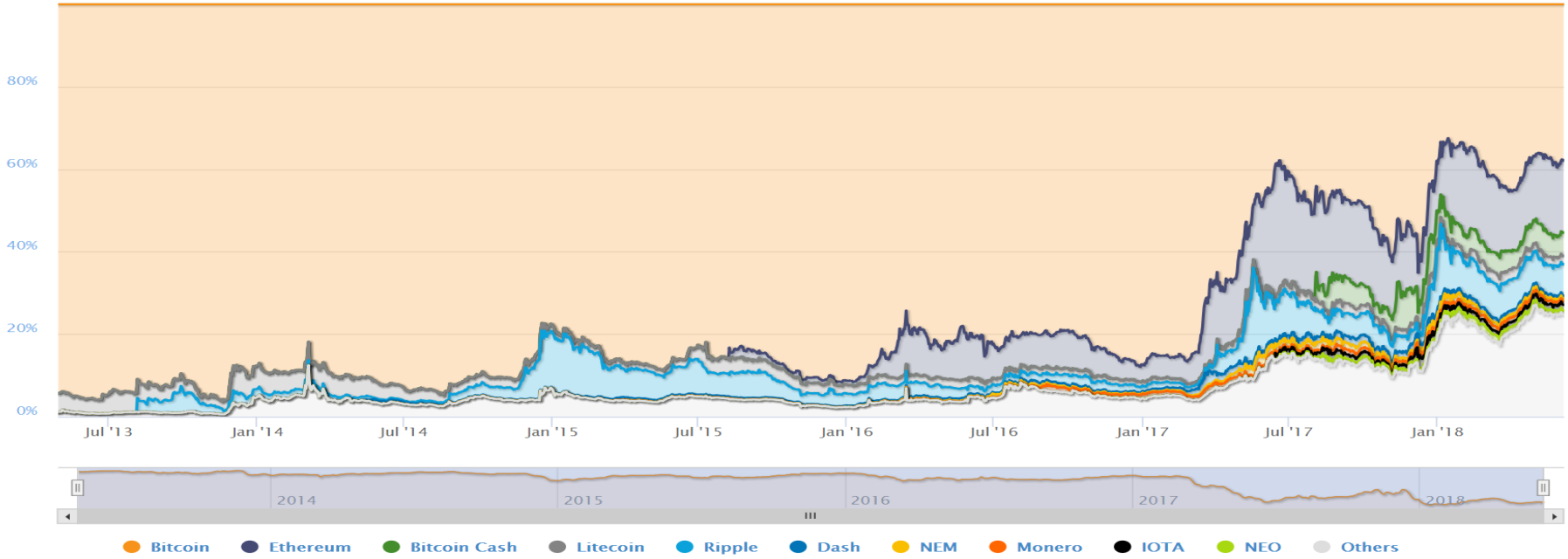
非中央集権を標榜した仮想通貨の取引の大本が、「信頼できる第三者」にならなければならないという矛盾。

非主流派の仮想通貨に対する51％攻撃を巡って

- 5月13日から15日にかけて、MonacoinがSelfish Mining攻撃を受け、ロシアの仮想通貨取引所に1000万円程度の被害が発生した。
- その後2週間ほどの間に、Bitcoin Gold、Verge、ZenCashといった仮想通貨も類似した攻撃を受け、各々、20億円、2億円、6000万円程度の被害が発生したと伝えられる。
- こうした攻撃の被害は、主として取引所に生じたが、同時に当該仮想通貨の相場を下落させることとなり、一般の仮想通貨投資家にも被害が及ぶこととなった。
- その攻撃方法は微妙に異なっているが、基本的には膨大なハッシュ計算能力を投入してブロックチェーンのマイニングを行い、攻撃者に都合の良いチェーンの分岐（fork）を発生させてそれをチェーンの本流にしてしまう攻撃であった。これらはいずれも、ハッシュ計算能力が攻撃者側に偏った場合に発生すると想定されていた「51%攻撃」のバリエーションであり、サトシ・ナカモトのBitcoin論文で存在が想定されていたものである。

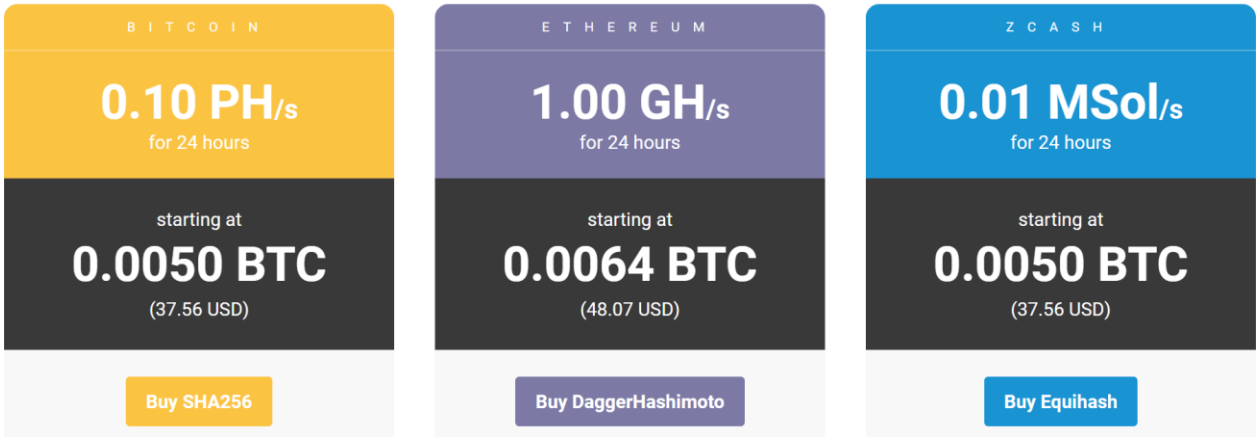
なぜ51％攻撃の被害が急増したか①

- 51%攻撃やそのバリエーションは、理論的にはその存在が指摘されていたが、膨大な費用が必要であり、実現性は低いと考えられていたが、最近、相次いで被害が発生している。その対象は、「非主流派」の仮想通貨である。
- この一つの原因は、非主流派の仮想通貨が高い価値を持つようになったこと。2017年後半からアルトコインが急速に値上がりし、主要な10通貨を除く「others」のシェアは、数%にとどまっていたものが、25%前後と大きなシェアを占めるに至っている。



なぜ51％攻撃の被害が急増したか②

- 非主流派の仮想通貨は、先行する主流派の仮想通貨との差別化を意識して構築され、例えば、既存のマイナーにマイニングされにくい特徴を持ったハッシュ関数を利用してきた。
- しかし、仮想通貨の数が増え、様々な主体がマイニングに参入するとともに、ハッシュ計算能力自体がインターネット上で売買されるようになる（www.nicehash.com）。
- ハッシュ計算能力自体がコモディティ化すると、非主流派がこれまでとってきた戦略では、攻撃を防ぐことができなくなる。主流派の仮想通貨用に利用されていた計算リソースを、非主流派のマイニングに転用が可能なのだ。



ハッシュ計算能力の時間貸しを考慮した攻撃難易度の試算

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$126.45 B	SHA-256	37,598 PH/s	*$699,965*	1%
Ethereum	ETH	$55.85 B	Ethash	207 TH/s	*$376,501*	2%
Bitcoin Cash	BCH	$16.89 B	SHA-256	3,644 PH/s	*$67,837*	14%
Litecoin	LTC	$6.68 B	Scrypt	281 TH/s	*$61,469*	7%
Monero	XMR	$2.50 B	CryptoNightV7	426 MH/s	*$28,643*	14%
Dash	DASH	$2.47 B	X11	1 PH/s	*$11,548*	41%
Ethereum Classic	ETC	$1.56 B	Ethash	9 TH/s	*$15,975*	56%
Bytecoin	BCN	$1.20 B	CryptoNight	490 MH/s	*$1,105*	79%
Zcash	ZEC	$1.01 B	Equihash	392 MH/s	*$53,033*	17%
Bitcoin Gold	BTG	$719.79 M	Equihash	27 MH/s	$3,677	249%
Bitcoin Private	BTCP	$451.39 M	Equihash	5 MH/s	$684	1337%
Dogecoin	DOGE	$387.29 M	Scrypt	190 TH/s	*$41,641*	11%
MonaCoin	MONA	$197.63 M	Lyra2REv2	2 TH/s	$3,577	734%
Electroneum	ETN	$156.21 M	CryptoNightV7	423 MH/s	*$28,401*	14%
ZenCash	ZEN	$119.63 M	Equihash	60 MH/s	$8,053	114%

（出典）https://www.crypto51.app/

シャドーは今回攻撃された仮想通貨。

９．中央銀行デジタル通貨を巡って

高まる中央銀行デジタル通貨の議論

中央銀行デジタル通貨を巡っては、世界各国の中央銀行において、様々な議論と立場の表明、実証実験から実際の発行まで、様々な取り組みが行われている。

中央銀行デジタル通貨（CBDC; Central Bank Digital Currency）という言葉やその定義は、使う人の立場によって区々である。DFC (Digital Fiat Currency)、DBM (Digital Base Money)、CBCC (Central Bank cryptocurrency)などの別名もある。

その使用する技術や実現形態も、次のように区々である。

１．民間の電子マネーと同様の技術を利用した中央集権的なシステムによるモバイルバンキングを中央銀行が運営するもの。

２．ビットコインのようにブロックチェーン技術を利用はするが、競争的マイニングは行わず、プライベート・チェーンで実装するもの。

３．民間のマイニング業者を巻き込み、競争的マイニングを行うパブリック・チェーンで実装するもの。

４．上記の技術のハイブリッドな組み合わせや、民間との連携、協業を想定しているもの。

中央銀行デジタル通貨の3つの系譜

こうした議論を全て紹介することはできないが、その議論の流れを整理するうえで、それらを次の3つの系譜に分けて整理することが可能であろう。

①先進主要国の中央銀行が、ビットコインの拡大に触発されて検討を開始した系譜。BIS/CPMIでの議論が広く知られており、様々な研究が進められているが、実装例はまだない。

②金融包摂の観点から始まったアフリカなど発展途上国での民間ベースの実装（M-PESA等）に中央銀行が関与することから始まった系譜。ITU-Tでアフリカ諸国を中心に議論されてきたが、中国、ロシア、インドなどが加入してきている。

③インフレ対策のためのドル化を進めてきた南米諸国の中央銀行が、新しくデジタル通貨を発行する系譜。いきなり実装されることが特徴。

Bitcoinのインパクト

ビットコインは確かに話題を集め、相場も高騰したが、金融の立場から見れば決済手段としての実用性は低く、まだまだ実験段階のものにすぎない。そんなビットコインが、金融業界に大きなショックを与えた。それは、ビットコインがインターネットを介して世界中で利用されたことに原因がある。

これまで、資金や証券に関する金融取引は、各国の金融当局によって規制されてきた。各国当局は、各々の国内法制によって事業者に免許を与え、各々の国内市場へのアクセスを許してきた。金融の国際化が進むにつれて、先進国間においては、国際的な資金や証券の取引が拡大したものの、金融取引が国境を越えるためには、電子的な情報のやり取りが大半を占めるにもかかわらず、国境に高い壁が築かれていたのである。

ところが、ビットコインはこの壁をやすやすと越えてみせた。インターネットに接続している利用者であれば、誰でもビットコインを購入し、売却することが原理的に可能である。実際、国際送金の手数料が高いのに対し、ビットコインを使って送金すれば安価に送金できることが喧伝された（最近ではこの手数料が高額になっているのだが）。

ビットコインの拡大は、金融の未来について様々な想像をかきたてた。もし既存の銀行券や銀行間の決済ネットワークが高コストで使いにくいのであれば、それらはインターネットで交換される仮想通貨にとってかわられるのではないか。真っ先に実証実験を行い、実績を積み重ねた担い手が、次世代のデファクト標準を握ることになるのではないか。そうした将来を見越して、従来は国境に守られて競争することのなかった中央銀行が、競争を始めたのだ。

各国中央銀行がデジタル通貨に関心

BANK OF ENGLAND

Staff Working Paper No. 605

The macroeconomics of central bank issued digital currencies

John Barrdear and Michael Kumhof

July 2016

Staff Working Papers describe research in progress by the author(s) and are published to elicit comments and to further debate. Any views expressed are solely those of the author(s) and so cannot be taken to represent those of the Bank of England or to state Bank of England policy. This paper should therefore not be reported as representing the views of the Bank of England or members of the Monetary Policy Committee, Financial Policy Committee or Prudential Regulation Authority Board.

Committee on Payments and Market Infrastructures

Digital currencies

November 2015

BANK FOR INTERNATIONAL SETTLEMENTS

BANK OF CANADA
BANQUE DU CANADA

Staff Working Paper/Document de travail du personnel 2016-42

On the Value of Virtual Currencies

by Wilko Bolt and Maarten R.C. van Oordt

Bank of Canada staff working papers provide a forum for staff to publish work-in-progress research independently from the Bank's Governing Council. This research may support or challenge prevailing policy orthodoxy. Therefore, the views expressed in this paper are solely those of the authors and may differ from official Bank of Canada views. No responsibility for them should be attributed to the Bank.

日本銀行スタッフによるサーベイ

日銀レビュー　2016-J-19

中央銀行発行デジタル通貨について
―　海外における議論と実証実験　―

決済機構局　小林亜紀子、河田雄次、渡邉明彦、小早川周司

Bank of Japan Review　2016 年 11 月

新しい情報技術を各種の金融サービスに活用していく「フィンテック（FinTech）」への関心が世界的に高まる中、中央銀行が自ら発行する通貨などに、こうした技術を活用する可能性についても、さまざまな議論や調査分析が行われている。とりわけ、最近では、フィンテックを代表する技術とされる「ブロックチェーン」や「分散型元帳技術」について、中央銀行が自ら実証実験を行う事例もみられている。日本銀行としては、これらの調査分析や実証実験などの動向を丹念にフォローしつつ、フィンテックを巡る国際的な議論に積極的に参画していく考えである。

① オランダ（オランダ銀行）

オランダ銀行は2016年3月、年次報告書の中で、ブロックチェーン・DLTを基に「DNBcoin」の試作品を開発する旨、公表している。その基本的な考え方について、同年6月の幹部講演では、ビットコインのソフトウェアを中央銀行が自ら試してみることにより、ブロックチェーンの機能についてより深く理解できるとしている。そのうえで、DNBcoinはあくまでオランダ銀行内部での試験に主眼をおいて開発されたものであり、広く一般に流通させる予定はないとしている。

② カナダ（カナダ銀行）

カナダ銀行は、2016年6月17日のウィルキンス副総裁の講演等において、商業銀行や民間企業と連携し、DLTの実験を行う旨、公表している。実験の概要については、各種フォーラム等の場でカナダ銀行のスタッフより説明がなされている。例えば本年10月に開催されたシカゴ連銀主催「シカゴ・ペイメンツ・シンポジウム2016」では、銀行間取引を再現した擬似環境のもとで、この実験に参加する民間金融機関がカナダ銀行の特別勘定に資金を担保として差し入れ、その見合いとしてカナダ銀行がDLTに基づく中央銀行債務（預金証券）を発行すると紹介されている。なお、カナダ銀行では、本実験の目的について、実験的な大口決済システム環境の中でDLTをテストすることを通じて、この技術のメカニズムや限界、可能性を理解することにある、としている。

③ 英国（イングランド銀行等）

英国では、2016年2月、ロンドン大学の研究者がイングランド銀行スタッフとの議論を経て、中央銀行発行デジタル通貨である「RSCoin」を提案する論文を公表している。このスキームでは、中央銀行と利用者の間に介在する複数の「ミンテッツ（mintettes）」と呼ばれる主体がRSCoinを発行・管理する上で一定の役割を果たすことが想定されている。すなわち、中央銀行はRSCoinの発行主体となる一方で、取引内容の精査、承認および関連する情報の中央銀行への送信といった処理は、複数のミンテッツに委託されることが想定されている。そのうえで、ミンテッツが適切に機能することを担保するため、中央銀行は取引検証を通じて生成されるブロックチェーンの「ブロック」の整合性を継続的に確認し、仮に不適切な処理を検知した場合には、そのような処理を行ったミンテッツを排除する仕組みとなっている。

また、イングランド銀行のカーニー総裁は、2016年6月の講演の中で、中央銀行のコア業務にDLTを活用することを検討する考えを明らかにしており、また、中央銀行デジタル通貨を巡る論点についても調査分析を行っているとしている。さらに、2016年9月、RTGSシステムの再構築に関する市中協議書の中で、DLTはまだ技術として成熟しておらずRTGSシステムに必要な極めて高水準の安定性を満たすにはいたらないものの、決済のあり方を変える潜在能力を秘めており、引き続き、学界、海外の中央銀行およびフィンテック企業とも連携して調査を行っていくとしている。

④ ロシア（ロシア銀行）

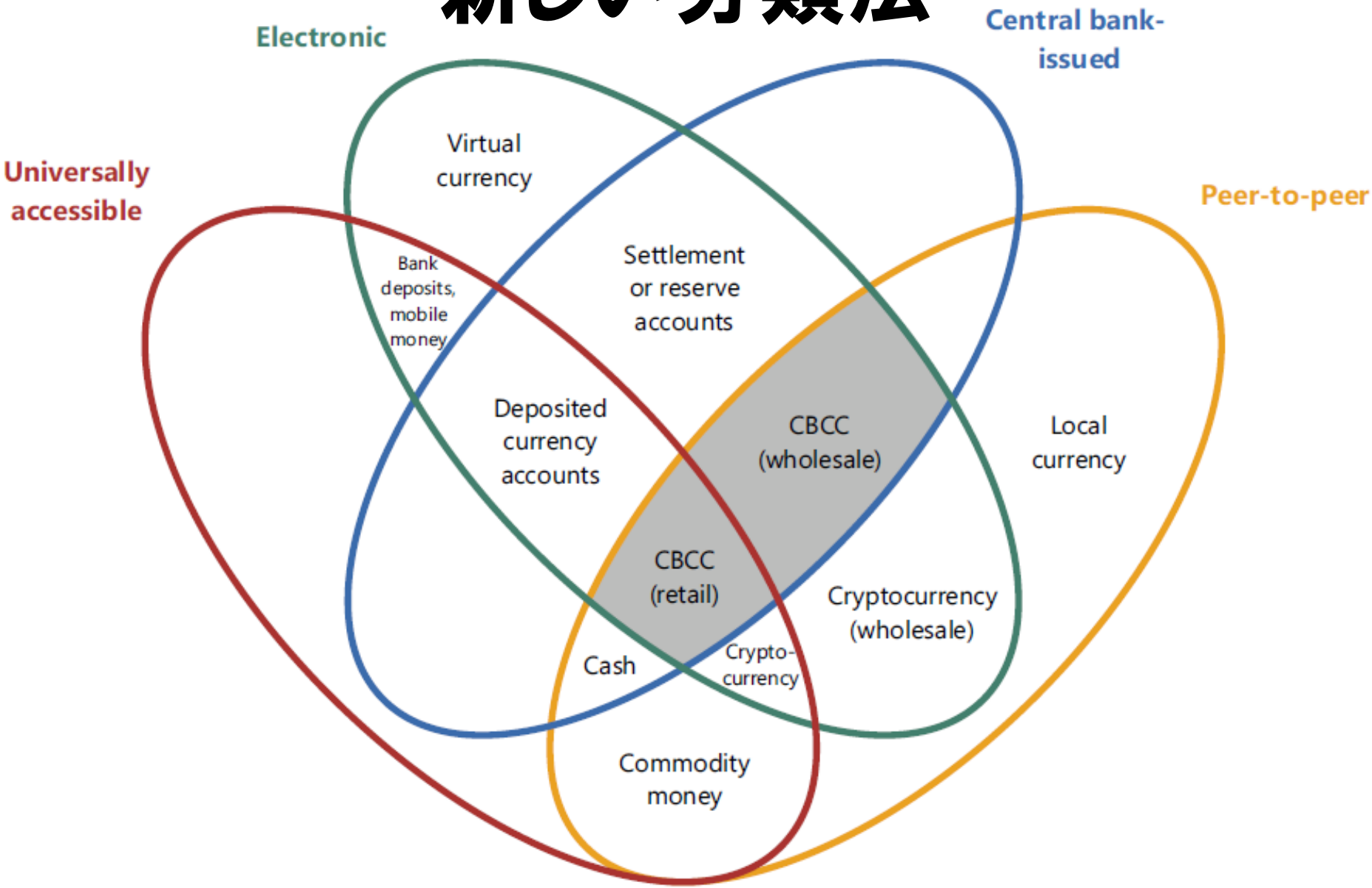
ロシア銀行は2016年10月、市場参加者と連携し、「Masterchain」というDLTを用いた金融情報伝達ツールの試作品を開発したと公表している。ロシア銀行のスコロボガトヴァ副総裁は、同試作品について、今後、ロシア銀行が立ち上げる「FinTechコンソーシアム」において検討を継続し、将来的には次世代金融インフラに活用することも検討すると発言している。

⑤ 中国（中国人民銀行）

中国人民銀行は現時点で、ブロックチェーン・DLTに関する実証実験を行っていると発表している訳ではない。その一方で、中国人民銀行は、中期的に自らデジタル通貨を発行する構想がある旨、対外的に明らかにしている。すなわち、中国人民銀行は2016年1月20日にデジタル通貨に関する検討会を開催し、専門家との間でデジタル通貨に関する意見交換を行っている。そのうえで、この検討会は、中国人民銀行のスタディグループが、国内外のデジタル通貨に関する研究成果等を取り込むとともに、中央銀行としてデジタル通貨に対する戦略目標をより一層明確にし、一日も早い中央銀行発行デジタル通貨の発表に向けて努力するよう求めている。

また、同行の范副行長は、2016年9月1日のブルームバーグ社への寄稿の中で、中国人民銀行が検討しているデジタル通貨の発行形態に関して、まずは、民間銀行に対して発行され、民間銀行が一般の顧客に対しその預入や払出に関するサービスを提供する、いわば「間接型」のアプローチの採用に傾いている旨述べている。本アプローチが望ましい理由について、范副行長は、現在の銀行券流通の枠組みを活用する方が、中央銀行発行デジタル通貨が紙の銀行券を徐々に代替していくことを容易にすると考えられることや、中央銀行発行デジタル通貨の管理に民間銀行も参加することは、リスク分散やイノベーション促進、実体経済への寄与や人々のニーズへの対応にも資するといった理由を挙げている。

新しい分類法



（出典）BIS Quarterly Review (September 2017)掲載CBCC論文

10. 金融庁における検討作業の進捗

金融審議会「金融制度スタディ・グループ」（平成29年11月29日開始）

情報技術の進展等の環境変化を踏まえた金融制度のあり方に関する検討

金融システムを取り巻く環境の変化

- ITの進展等により、金融サービスを個別の機能に分解して提供（アンバンドリング）・複数のサービスを組み合わせて提供（リバンドリング）する動きが拡大
- ファンド等の主体による、銀行に類似した金融仲介（シャドー・バンキング）が拡大
- 金融環境が変化する中、多くの金融機関はビジネスモデルの再構築を図っているが、その際、制度面での障害があれば、除去していく必要
- さらに、将来的には、デジタル通貨の出現等が金融システムを大きく変革させる可能性

現行法制の特徴と課題

① 業態ごとに法令（業法）が存在し、機能・リスクが類似したサービスでも、行為主体（業態）によってルールが異なる

- 業態をまたいだビジネス選択の障害となりかねない
- 規制が緩い業態への移動や業態間のすき間の利用等を通じ、規制を回避する動きが生じかねない

② 金融に関する統一的な基本的概念・ルールが存在しない

- 「金銭」等の基本的概念に変化が生じた場合などに、各業法を個別に改正して対応する必要

③ 各業法に、環境の変化に対応していない規制が存在する可能性

- ITを活用した合理化やITに対抗した合理化などが、固有の規制によって円滑に実現できない可能性

検討の方向性

① 同一の機能・リスクには同一のルールを適用

- 例えば、金融の機能を、「決済」「資金供与」「資産運用」「リスク移転」などに分類し、機能・リスクに応じたルールの適用を検討

② 金融に関する基本的概念・ルールを横断化

- 金融規制における定義の横断化の検討

③ 環境の変化に対応すべく規制を横断的に見直し

金融庁「仮想通貨交換業等に関する研究会」（平成30年4月10日開始）

「仮想通貨交換業等に関する研究会」の設置について

2018年３月８日
金　　融　　庁

１．趣旨

仮想通貨に関しては、マネーロンダリング・テロ資金供与対策に関する国際的要請がなされたことや、国内で当時世界最大規模の仮想通貨交換業者が破綻したことを受け、2017年４月より、仮想通貨と法定通貨等の交換業者に対し、登録制を導入し、本人確認義務等の導入や説明義務等の一定の利用者保護規定の整備を行った。

その後、コインチェック株式会社が、不正アクセスを受け、顧客からの預かり資産が外部に流出するという事案が発生したほか、立入検査により、みなし登録業者や登録業者における内部管理態勢等の不備が把握された。また、仮想通貨の価格が乱高下し、仮想通貨が決済手段ではなく投機の対象となっている中、投資者保護が不十分であるとの指摘も聞かれる。さらに、証拠金を用いた仮想通貨の取引や仮想通貨による資金調達など新たな取引が登場しているという動きも見られる。

こうした状況を受け、仮想通貨交換業等をめぐる諸問題について制度的な対応を検討するため、「仮想通貨交換業等に関する研究会」を設置する。