

2018年1月26日

仮想通貨の動向

京都大学 公共政策大学院
岩下 直行

目次

- 1. Bitcoin価格の高騰と停滞**
- 2. Bitcoin取引の実際とそのリスク**
- 3. Bitcoinの誕生とその前史**
- 4. 仮想通貨市場の現状**
- 5. ICOの増加と仮想通貨の高騰の背景**
- 6. Blockchain 2.0 と the DAO事件**
- 7. 中央銀行デジタル通貨を巡って**

1. Bitcoin価格の高騰と停滞

ビットコイン先物、CMEとCBOEで取引可能に

2017年12月2日 / 00:29

[ワシントン／ロンドン 1日 ロイター] 米商品先物取引委員会(CFTC)は1日、米先物取引所運営大手のCMEグループ(CME.O)と、シカゴ・オプション取引所(CBOE)を運営するCBOEグローバルマーケット(CBOE.O)に、仮想通貨ビットコインの先物上場を認める方針を公表した。

米国の伝統的な取引所でビットコイン関連の金融商品の取引が認められるのは初めて。今後ビットコインに対する当局の規制は強まることが予想される。

CMEは、ビットコイン先物を12月18日に上場するとした上で、現物市場に沿って値づけ・清算を行うとした。CBOEは同先物の上場日を決めていない。CMEとCBOEは当初証拠金として35－40%を要求するなど、通常よりも厳格なリスク管理を行う見通し。

CME Group Inc



仮想通貨プラットフォーム、クリプトコンペアの最高経営責任者(CEO)は今回の発表について「デジタル資産が主流であることが暗に認められた」とした上で、将来的に上場投資信託(ETF)などの取引につながる可能性もあると述べた。

ビットコインはこの日、ルクセンブルクに本拠を置くビットスタンプBTC=BTSPで6.4%高の1万0580ドル。公表後20分間で5%強値上がりした。



(9カ月前の)Bitcoinの価格と利用者数の推移



Bitcoinの価格の長期時系列

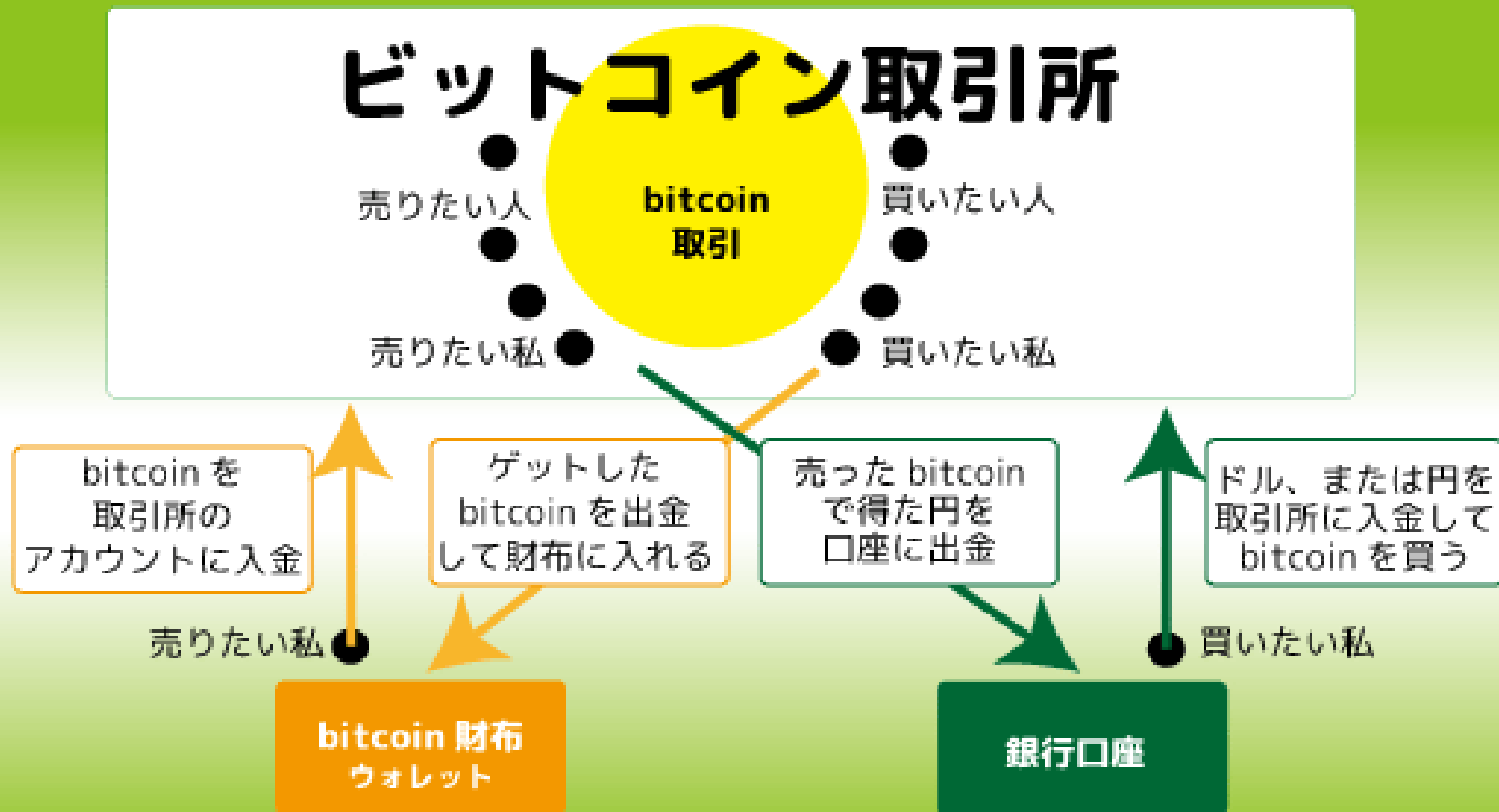


Bitcoinの価格の最近1か月の動き



2. Bitcoin取引の実際とそのリスク

ビットコイン取引所での売買のイメージ



ビットコインの秘密鍵の管理方法による分類

1. ウォレットアプリ

PCやスマートフォンのウォレットアプリをダウンロードし、秘密鍵を自分で管理する方式。自分で管理しているので安心だが、デバイスの故障で秘密鍵を復旧できなくなるリスクや、マルウェア感染等によって秘密鍵が露見してビットコインが不正に送金されるリスクがある。

2. ウォレットサービス

サーバー型のオンライン・ウォレットサービスに登録し、業者に暗号通貨の管理を委託する方式。

サーバー型サービスはデバイスを選ばず、インターネットに繋がってさえいればどこからでもアクセスでき、送金や残高の確認ができるが、業者が不正を働いたり攻撃を受けて預けてあるビットコインが奪われるリスクがある。

3. ハードウェアウォレット

USB等のフラッシュメモリやハードウェアウォレットに秘密鍵や、秘密鍵を復元するパスワードを保存する方式。

4. ペーパーウォレット

紙などの物理媒体に秘密鍵や秘密鍵の情報が含まれたQRコード、秘密鍵を復元するためのパスワードを転写して保存する方式。

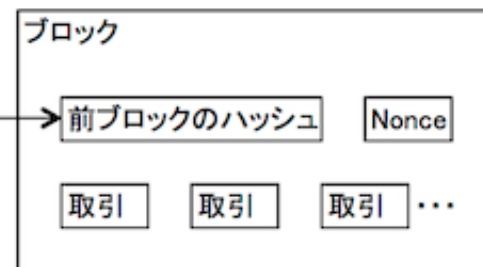
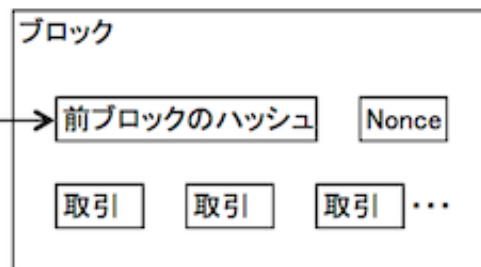
Bitcoinの発掘の仕組み

Bitcoin

The magic of mining

Minting the digital currency has become a big, ru

Jan 10th 2015 | BODEN, SWEDEN | From the print edition



ビットコインは発行主体を持たず、インターネット上のP2Pネットワークで情報が共有される。誰でも利用者となることができ、ソースコードや取引履歴の検証を可能とすることで、信頼を確保。計算能力を提供してシステム全体の維持管理に貢献すること(=発掘)に対し、一定の報酬が与えられる。この報酬を求めて、専門業者が膨大な計算能力を投入して「発掘」を進めている。



ビットコイン採掘時の各ノードの役割

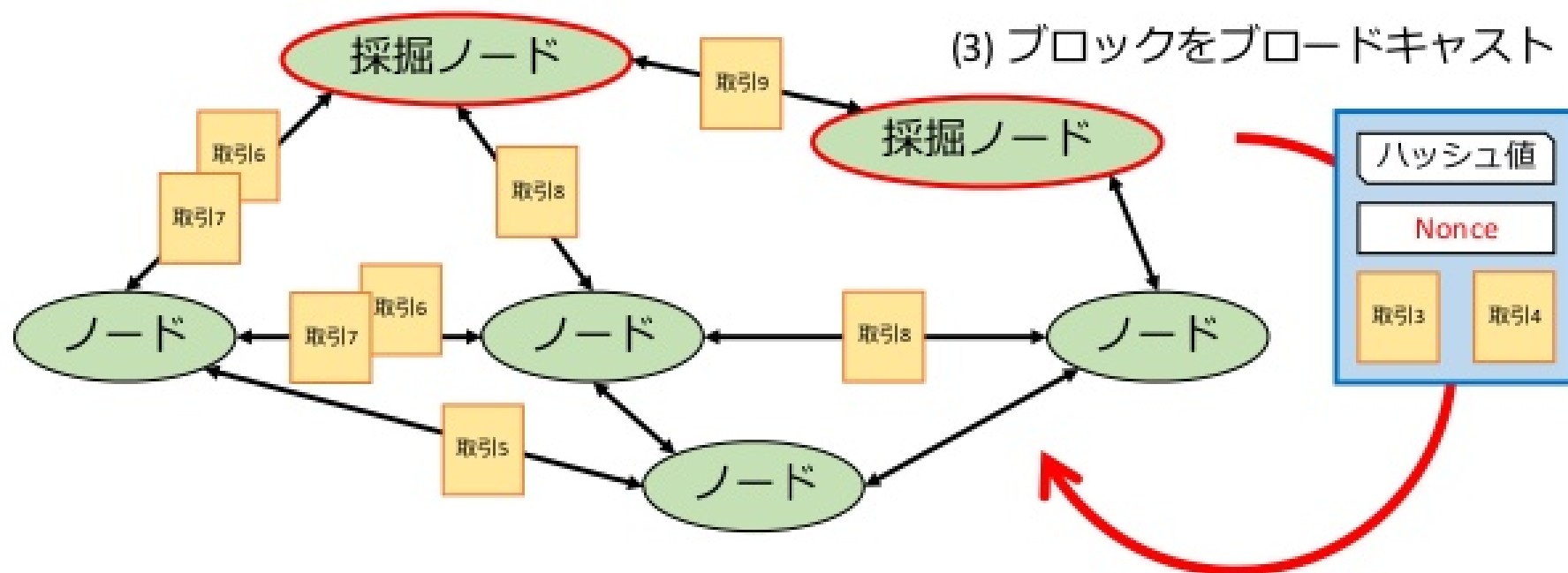
Proof-of-work

18

(1) 各ノードは常に新しい取引情報をブロードキャスト

(2) 採掘ノードは常に採掘処理を実行

(3) ブロックをブロードキャスト



ネットワーク全体で取引の正しさを監視

(4) 各ノードはブロックを検証

3. Bitcoinの誕生とその前史

Satoshi Nakamoto論文 (2008年)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

2009年1月9日のメール

Bitcoin v0.1 released

Satoshi Nakamoto | Fri, 09 Jan 2009 17:05:49 -0800

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:

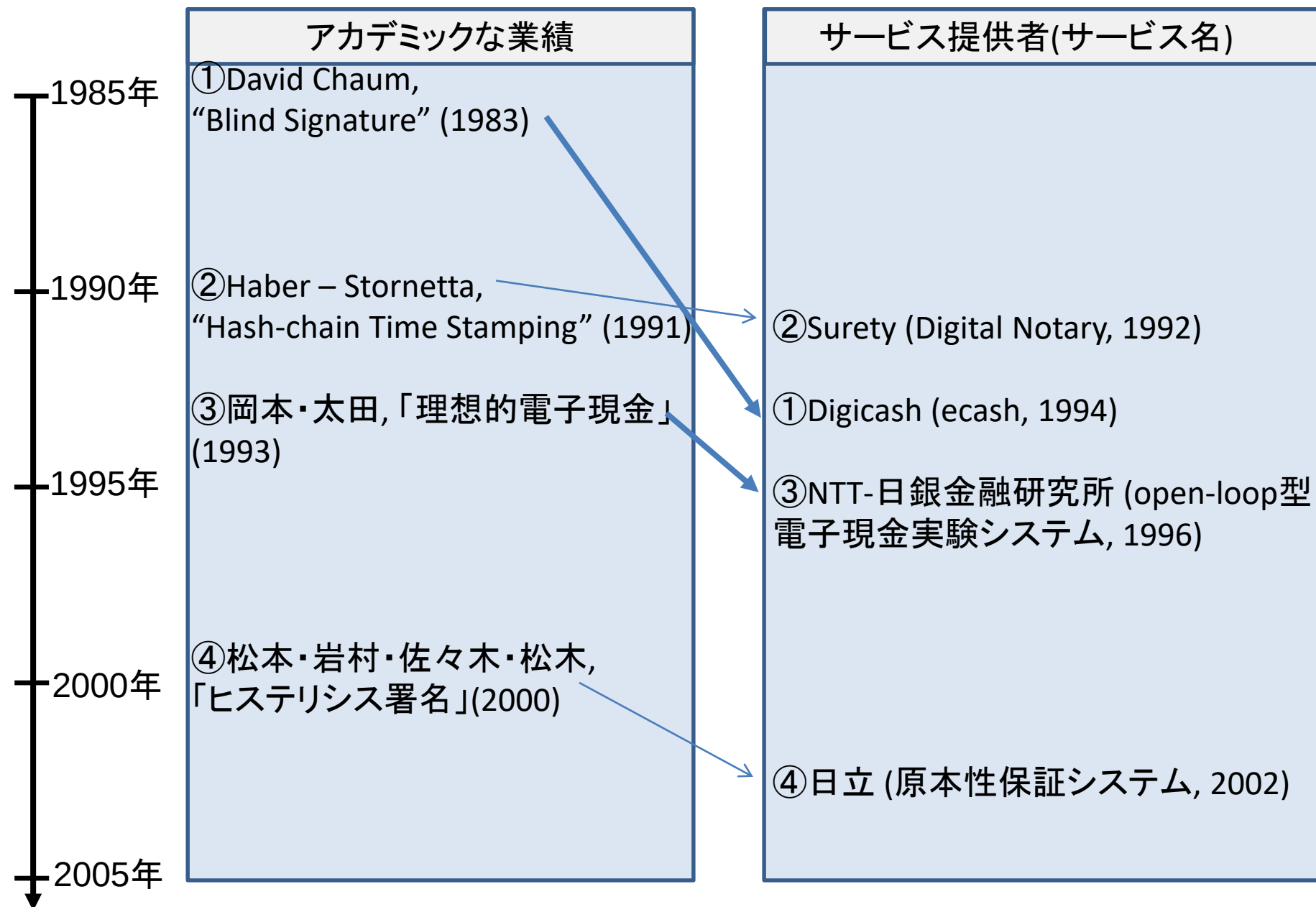
<http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar>

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

If you can keep a node running that accepts incoming connections, you'll really be helping the network a lot. Port 8333 on your firewall needs to be open to receive incoming connections.

Bitcoinに先立って開発されていた主な技術



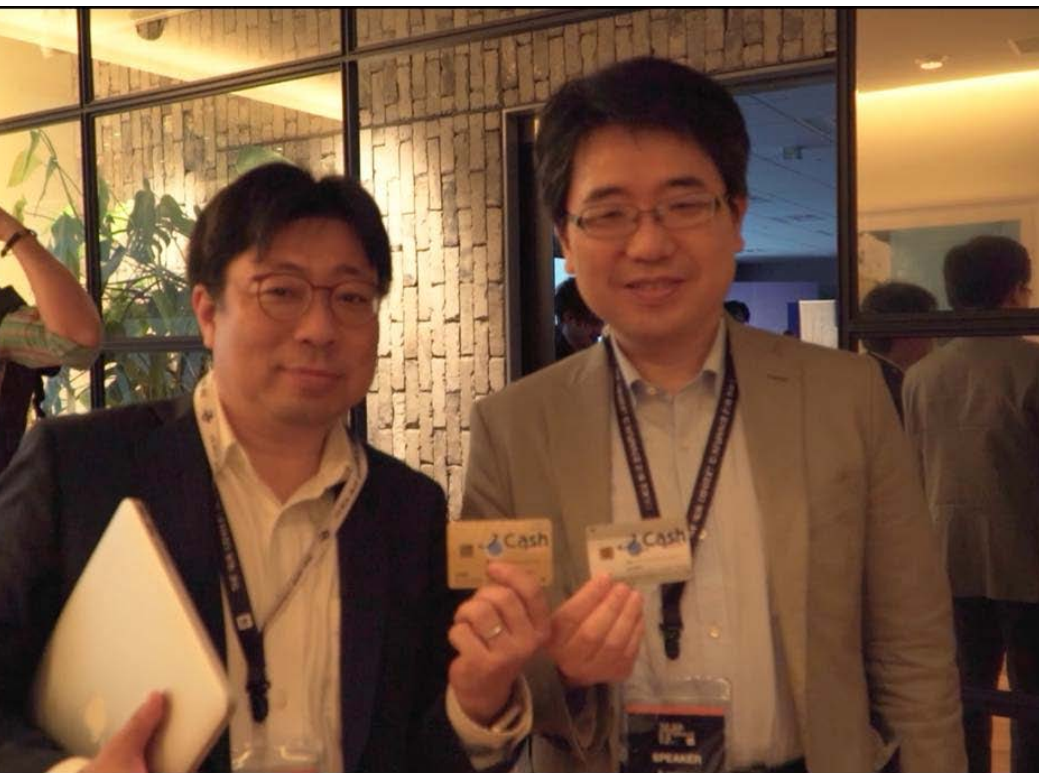


岩下 直行

11月1日 10:56 · 🌐 ▼

ジョージタウン大学教授に就任された松尾先生の投稿写真です。インターネットキャッシュは当時としては先進的すぎて拡大しなかったのですが、その後の日本の交通系電子マネーの発展や、更にその後の仮想通貨の研究に少なくない影響を与えたトライアルでした。写真のコメントもご参照下さい。

<https://www.facebook.com/naoyuki.iwashita.kyoto>



Shin'ichiro Matsuo

日時: 2016年7月19日 場所: サンノゼ (アメリカ合衆国・California)付近 · 2人 ▼

○ タイムラインに表示 ▼

We were the e-cash pioneers at 1998-2000 Bank of Japan-NTT e-cash experiment. The smart card Iwashita-San has is for step1 and I have is for step2 of that project. At that e-cash protocol, offline transfer, open loop, multi-currencies and transfer using email attachment were already realized. It was about 18 years ago. This photo at the new context conference 2016 is a historical shot and this opportunity is the start line of new generation of financial cryptography.

翻訳を見る

— 友達: 岩下 直行

Bitcoinの誕生前史を読み解くと

- Bitcoinが考案される前から、Bitcoinの特徴である
 - ① 乱数とデジタル署名による電子的な価値の表象、
 - ② 分割可能性、open-loop性、匿名性の付与、
 - ③ ハッシュ関数や署名のchainによる改竄防止、については、様々な技術が考案され、実装されていたことが分かる。
- しかし、システムリソースの不足やコスト、利便性の問題から、当時はそれらの技術が広く普及することはなかった。
- ecashは既存の通貨建てで発行された「電子マネー」的なものであったが、Chaumian digital cashと呼ばれる模倣プロジェクトの中には、独自の通貨単位を導入した、現在の「仮想通貨」に似たものもあった。それらは全て、特に注目されることもなく消滅している。

何故Bitcoinが「成功」したのか

① peer-to-peerによる分散コンピューティングの採用

— CPU、ストレージ、通信のコスト低下によって、一般ユーザーが保有するインターネット上のリソースだけで稼働可能になった。

② 競争的マイニングによる非中央集権化(de-centralized)

— 署名検証、二重使用チェックなどの機能を果たす参加者に報酬を付与し、その役割を果たせることの証明のために、一定の条件を満たすハッシュ値の探索を行わせる仕組み(Proof of Work)を導入。

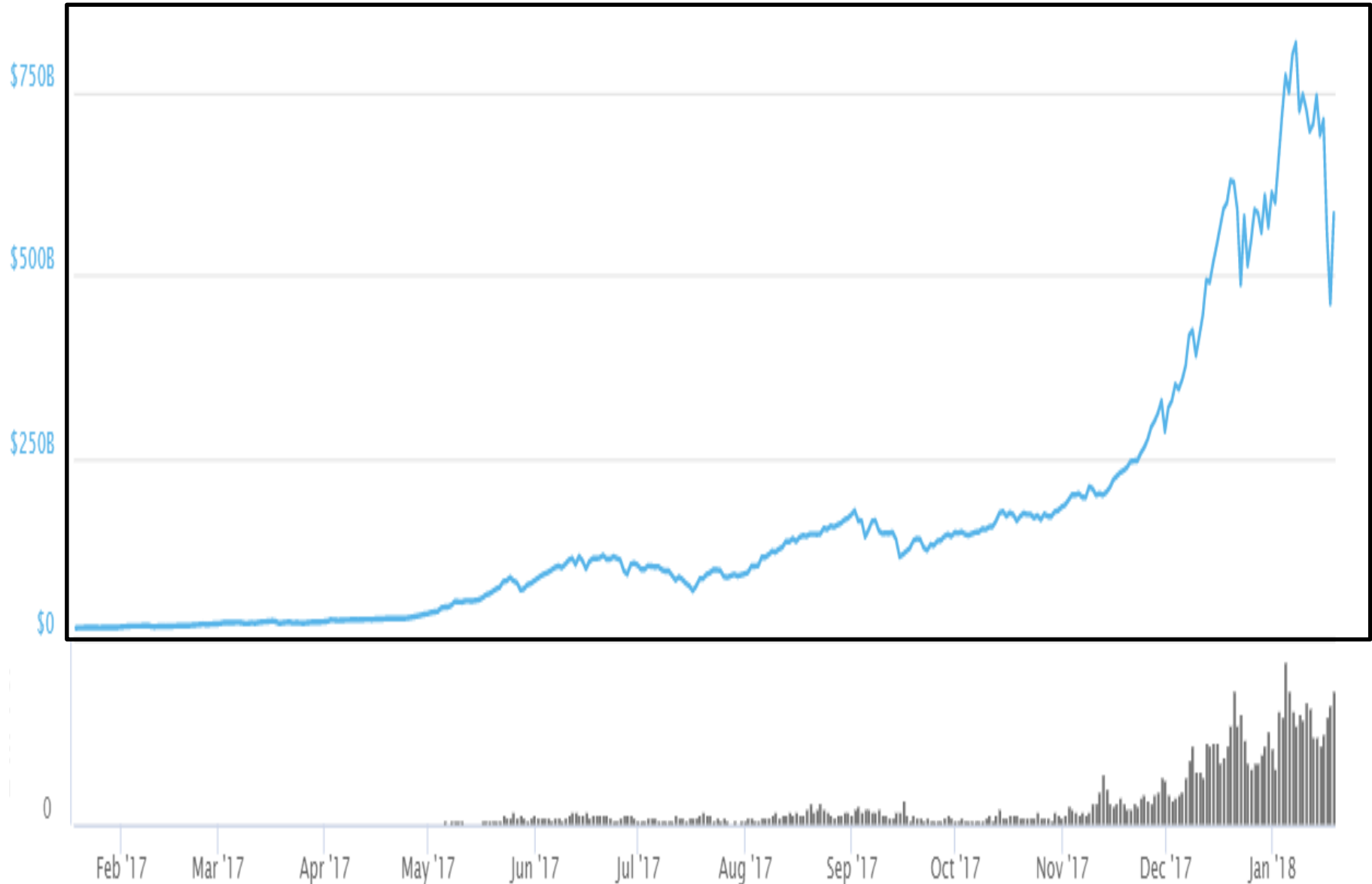
③ 独自通貨単位(BTC)の採用による投資機会の提供

— 決済手段として用いるのであれば法定通貨建ての方が便利だが、交換価値を維持する費用が掛かる。システムを支えるマイニングの報酬の分だけ、仮想通貨を追加発行して賄うことで、外部からの費用投入なしにシステムを維持することが可能になった。

⇒ システム維持費用の「自給自足」が可能な仕組みを構築できたことが、現在の「成功」の一因と考えられる。

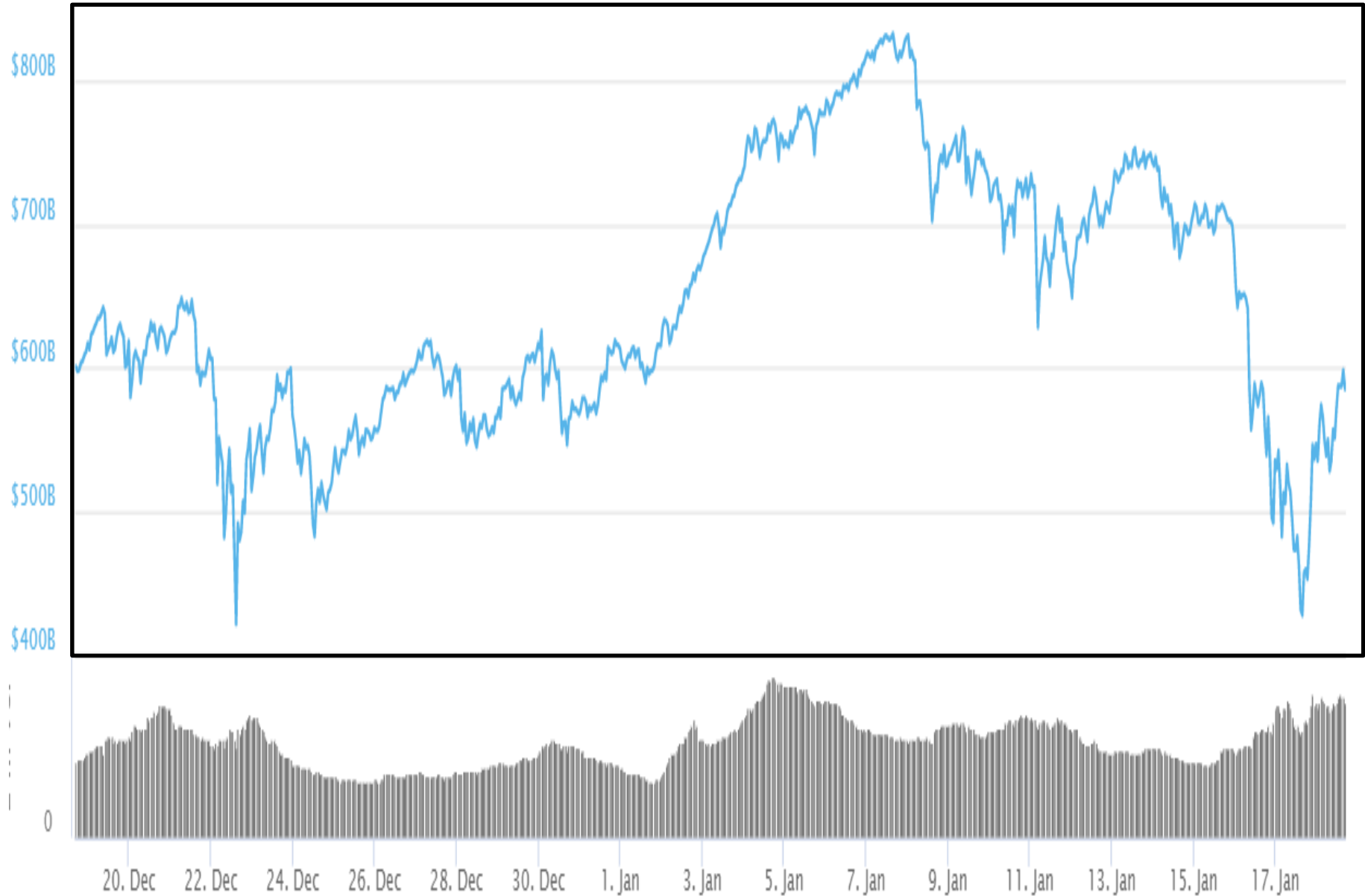
4. 仮想通貨市場の現状

全仮想通貨の時価総額の推移（1年間）



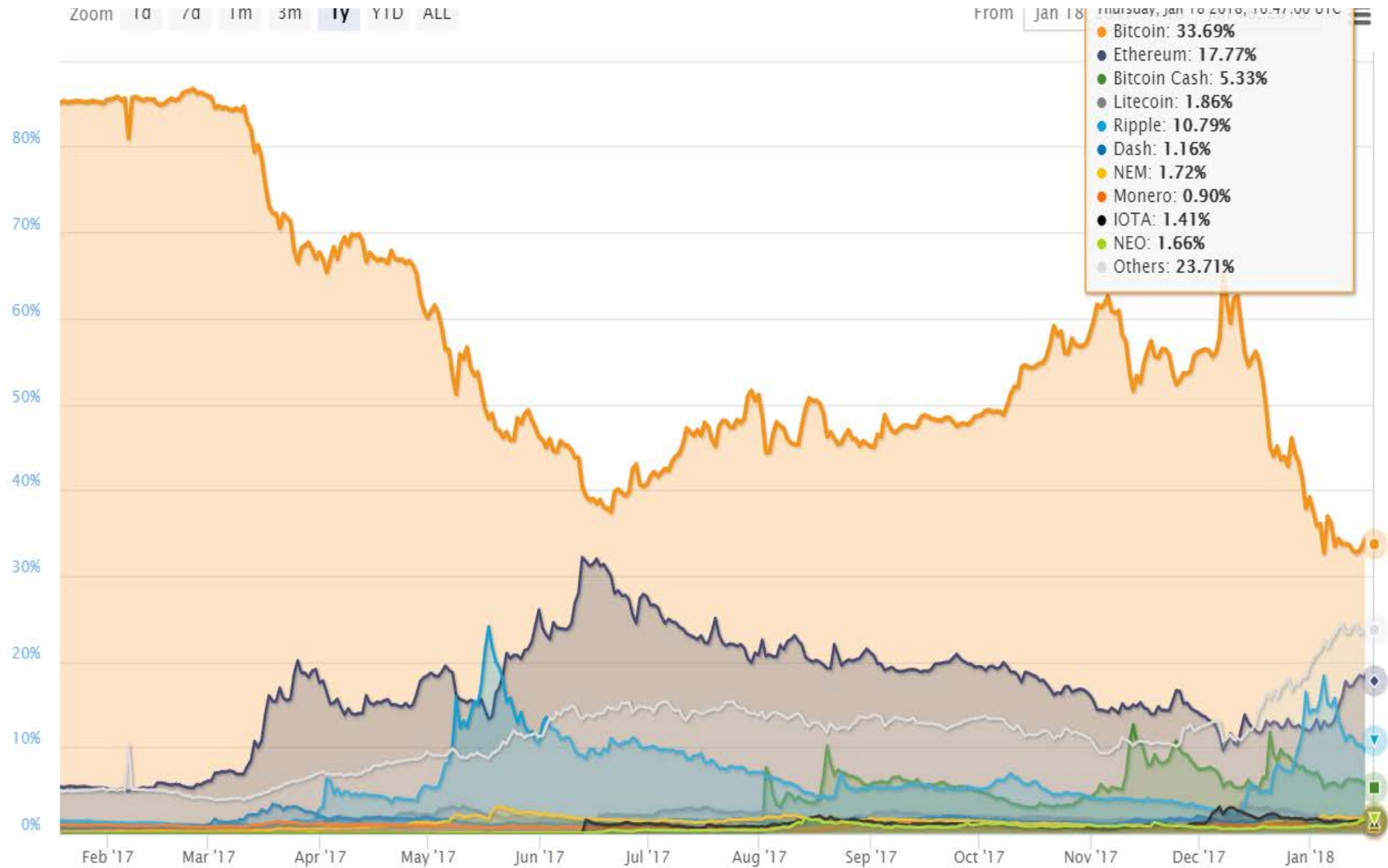
(出所) coinmarketcap.com

全仮想通貨の時価総額の推移（1か月）



(出所) coinmarketcap.com

仮想通貨の時価総額のシェアの推移(1年間)



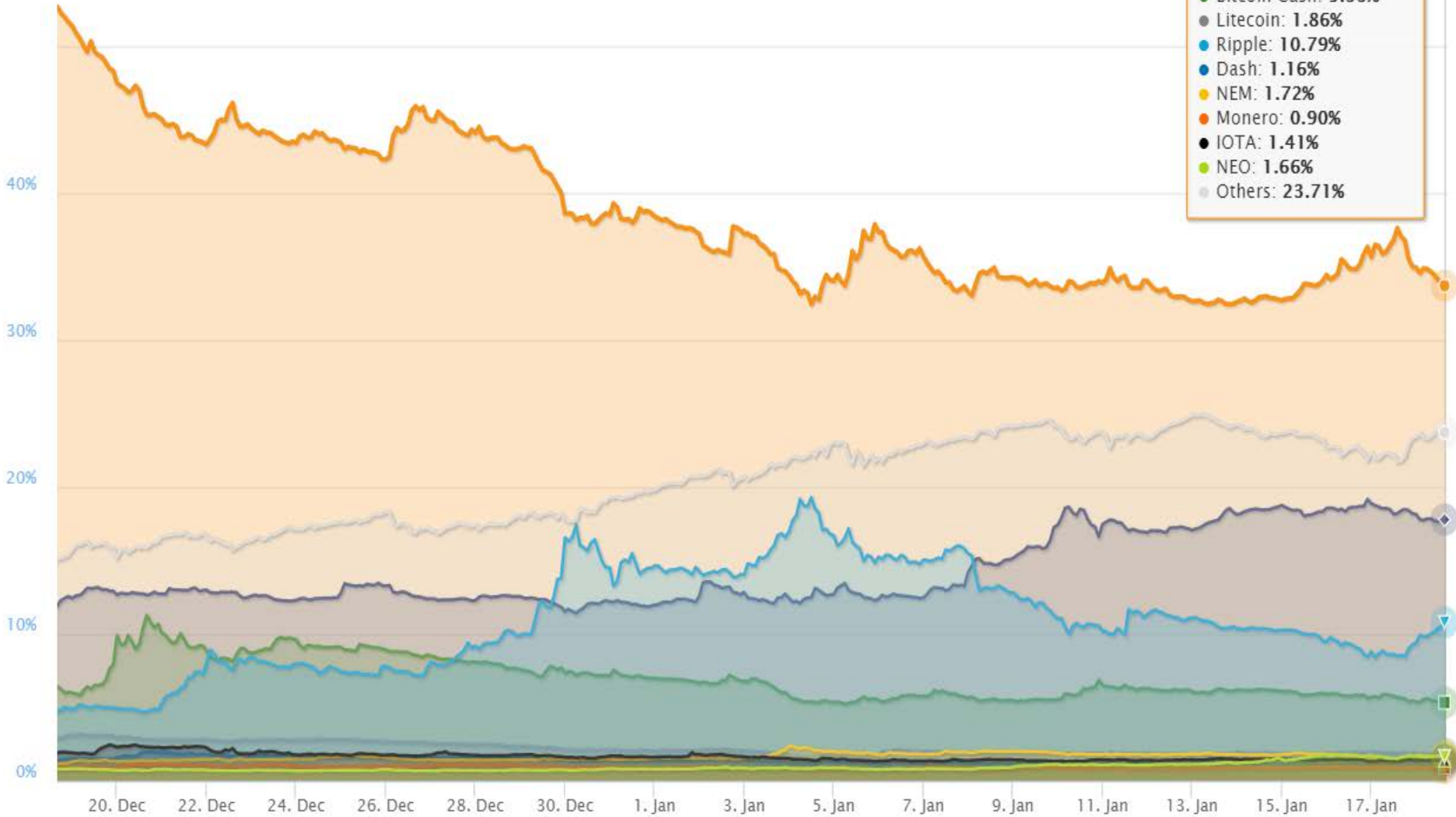
(出所) coinmarketcap.com

仮想通貨の時価総額のシェアの推移(1か月)

Zoom 1d 7d 1m 3m 1y YTD ALL

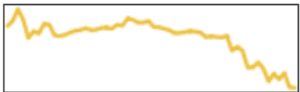
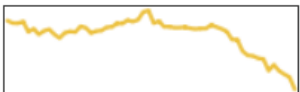
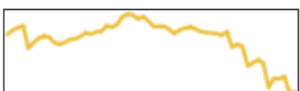
From Dec 18, 2017 Thursday, Jan 18, 16:00-17:00

- Bitcoin: 33.69%
- Ethereum: 17.77%
- Bitcoin Cash: 5.33%
- Litecoin: 1.86%
- Ripple: 10.79%
- Dash: 1.16%
- NEM: 1.72%
- Monero: 0.90%
- IOTA: 1.41%
- NEO: 1.66%
- Others: 23.71%



(出所) coinmarketcap.com

仮想通貨の時価総額上位10銘柄

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$164,787,072,974	\$9,803.86	\$15,273,300,000	16,808,387 BTC	-18.48%	
2	 Ethereum	\$79,967,818,151	\$824.10	\$6,496,390,000	97,036,664 ETH	-25.88%	
3	 Ripple	\$37,101,368,070	\$0.957723	\$4,888,990,000	38,739,142,811 XRP *	-31.17%	
4	 Bitcoin Cash	\$25,045,890,637	\$1,480.55	\$1,253,900,000	16,916,613 BCH	-25.13%	
5	 Cardano	\$12,257,515,211	\$0.472769	\$1,157,680,000	25,927,070,538 ADA *	-27.10%	
6	 Litecoin	\$8,382,067,677	\$152.97	\$1,129,020,000	54,796,933 LTC	-24.82%	
7	 NEO	\$6,558,825,000	\$100.91	\$1,014,380,000	65,000,000 NEO *	-33.77%	
8	 NEM	\$6,555,716,999	\$0.728413	\$137,183,000	8,999,999,999 XEM *	-35.81%	
9	 Stellar	\$5,916,957,830	\$0.330726	\$335,169,000	17,890,815,448 XLM *	-31.84%	
10	 IOTA	\$5,807,661,755	\$2.09	\$203,085,000	2,779,530,283 MIOTA *	-30.38%	

(出所) coinmarketcap.com

5. 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、イーサリウ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.

TOP 10 ICOs の変化

2016年のTOP 10



2017年のTOP 10

順位	プロジェクト名	資金調達額(ドル)
1	Waves	\$16,436,095
2	Iconomi	\$10,576,227
3	Golem	\$8,596,000
4	SingularDTV	\$7,500,000
5	Lisk	\$5,700,000
6	Digix DAO	\$5,500,000
7	FirstBlood	\$5,500,000
8	Synereo	\$4,700,000
9	Decent	\$4,178,357
10	Antshares/NEO	\$3,608,378

2016年計

件数46件 調達額 \$96,389,917

順位	プロジェクト名	資金調達額(ドル)
1	Filecoin	\$257,000,000
2	Tezos	\$232,319,985
3	EOS Stage 1	\$185,000,000
4	Paragon	\$183,157,275
5	Bancor	\$153,000,000
6	Kin	\$97,041,936
7	Status	\$90,000,000
8	TenX	\$64,000,000
9	MobileGO	\$53,069,235
10	KyberNetwork	\$48,000,000

2017年10月まで計

件数201件 調達額 \$3,256,704,359

Tezos(テゾス)ICO「持ち逃げ疑惑」で創業者、スイス基金らが米国の投資家から集団訴訟された 米証券法違反の可能性も ICOバブル崩壊?

2017年11月04日 19:54

今年最大のICO(イニシャル・コイン・オファリング)で2.32億ドルを調達した**Tezos(テゾス)**の創業者、キャスリーン・ブライトマンと夫のアーサー・ブライトマン、そしてICOの「受け皿」となったスイスの基金らが、米国の投資家から集団訴訟されました。



提訴したのはこのICOに応募した投資家、アンドリュー・ベーカーで、弁護士事務所はサンディエゴのテイラー・コーブランドです。訴状では被告が米国証券取引法に違反し、未登録の証券を販売したとしています。

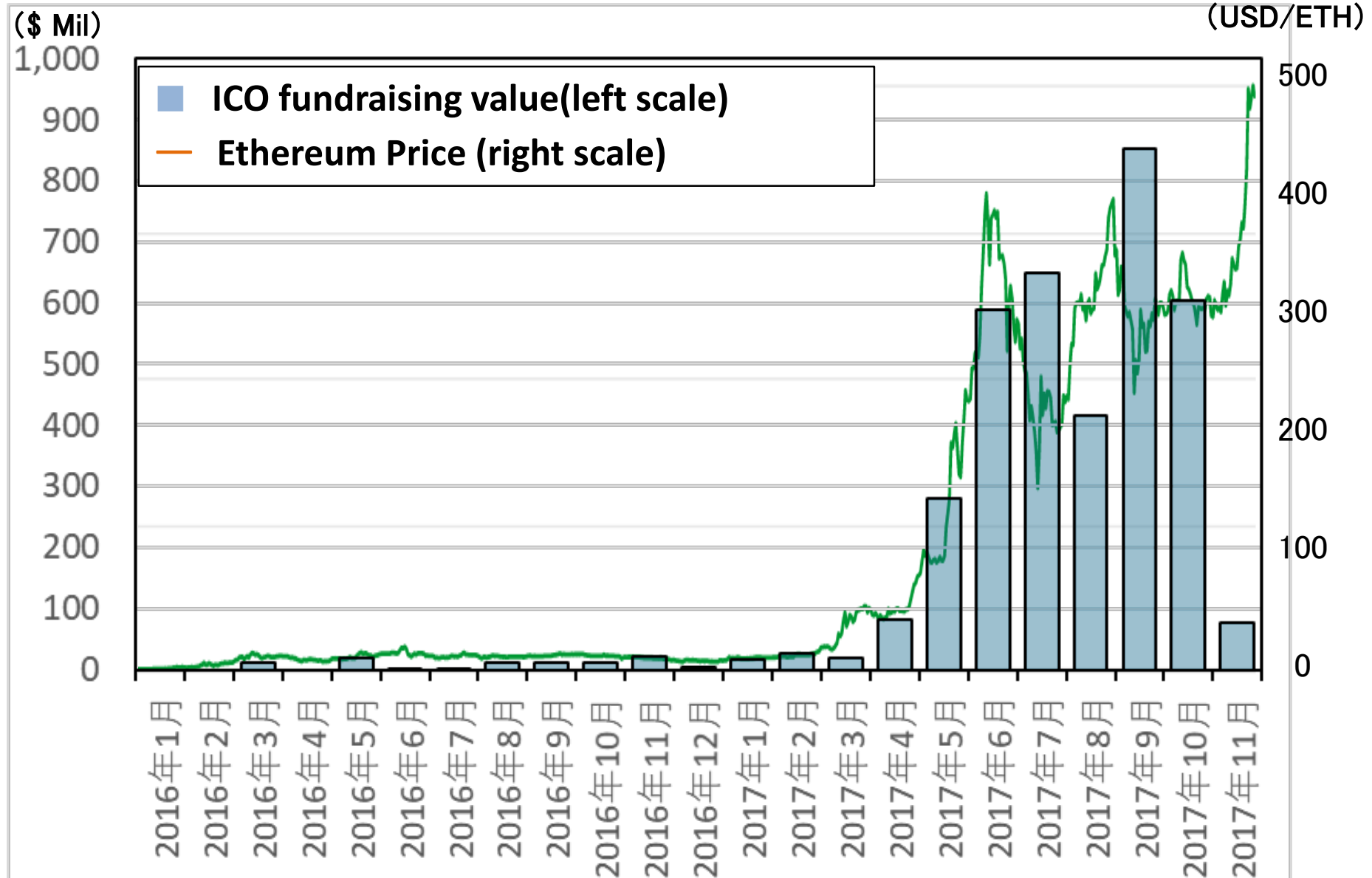
今回の訴訟に先立ち、テゾスの創業者と、ICOの投資家のおカネの送金先であるスイスの基金との間で揉め事が起きている事は、以前、紹介しました。今回の訴訟は、スイスのズーク郡の法律を活用した「シュティットウング・モデル」と呼ばれるICOの手法が、米国の証券法に抵触するのではないか？ というテスト・ケースです。

今回訴訟を起こしたのが米国人なので、SECがExtraterritorial appropriationと呼ばれる権限を発動するかどうかにも注目されます。アメリカの証券法では、いくらICOがスイスで行われても、それがアメリカ人に販売されれば米国証券取引法が適用されるとされているからです。

テゾスには日本の投資家も多数応募していると思います。しかし皆さんが仮想通貨でスイスの基金に送金したおカネは、「寄付」という法的位置づけであり、それを取り返すことは出来ない仕組みになっています。だから内紛や訴訟で、いつまでたってもテゾス・トークンが貰えないということになると、投資家が送金したおカネは、最悪の場合、戻ってこないのです。

今回のケースの展開如何では、ICOバブルが崩壊する可能性もあるので、注意深く見守りたいと思います。

ICOによる資金調達額とイーサリアム価格の推移



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

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

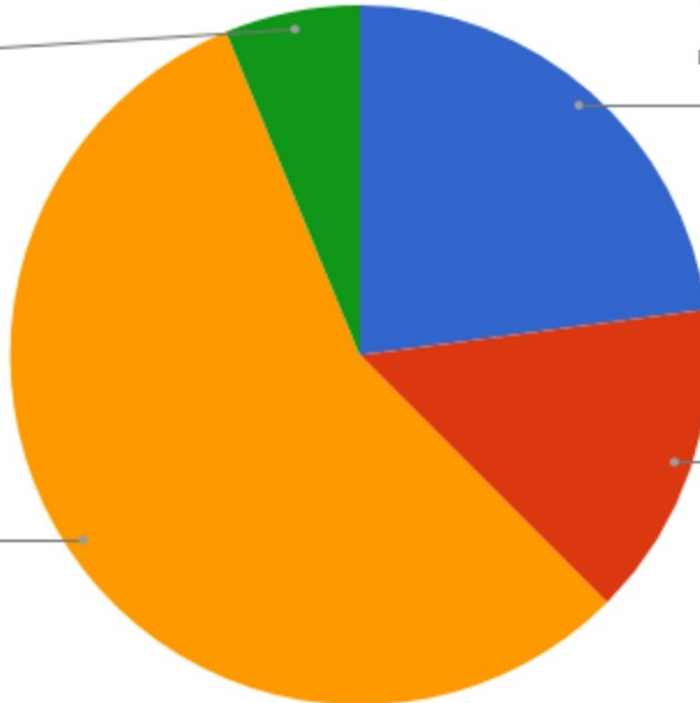
Product delivery

Working product
6.3%

Alpha
22.9%

Beta
14.6%

No product
56.3%



ICOはヘッジファンドの最も確実な金儲け法

Hedge Funds Flip ICOs, Leaving Other Investors Holding the Bag

By Olga Kharif (Bloomberg.com, 2017年10月4日 0:21 JST)

..one of the surest ways to get rich quickly with cryptocurrencies is to be in early on initial coin offerings.

Hedge funds are proving to be first among equals when it comes to digital token sales by technology startups, receiving preferential discounts and terms and then often cashing out.

“It’s not healthy for the ecosystem, and it’s pretty abusive,” said Kyle Samani, a managing partner at Austin, Texas-based Multicoine Capital, which invests in ICOs. “They are getting a discount because they are a big name, and they think it’s going to draw the retail investor. It’s the greater fools theory -- I’ll buy it if there’s someone who’s more of a fool than me.”

米国SEC(証券取引委員会)の検討結果の公表



U.S. SECURITIES AND
EXCHANGE COMMISSION

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," "Token Sales," "White Paper Offerings," and "Digital Asset Offerings."

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・売上に該当し得るとの見解を表明。

米SEC、仮想通貨資金調達(ICO)2件を詐欺で告発

今日(米国時間10/01)証券取引委員会(SEC)は、ダイヤモンドおよび不動産の仮想通貨資金調達(ICO)を、投資家を欺いたとして告発した。

初の仮想通貨に基づく不動産会社であるREcoin、およびダイヤモンド会社のDRC

Worldは、いずれもMaksim Zaslavskiyという実業家が所有している。SECは声明文で、これらの会社が未登録証券および、実在しないコインを無防備な投資家に販売したとして、Zaslavskiyを告発した。

SECによると、Zaslavskiyは投資家らに、この取引で「膨大なリターン」が期待できると話し、集めた資金が投資される方法やすでに投資された金額を偽って伝えた疑いがある。その後米国政府は緊急裁判命令を発行し、Zaslavskiyと所有する会社の資産を凍結させた。これは、仮想通貨に基づく資金調達(ICO: Initial Coin Offering)が詐欺で告発された最初の事例ではなく、間違いなく最後でもない。

..

(出典)TechCrunch Japan 2017年10月02日



MAS(シンガポール通貨庁)がICOの規制を表明



Email Subscription | FAQs | Contact Information | Feedback | Si

Search

SE

MAS clarifies regulatory position on the offer of digital tokens in Singapore

Singapore, 1 August 2017... The Monetary Authority of Singapore (MAS) clarified today that the offer or issue of digital tokens in Singapore will be regulated by MAS if the digital tokens constitute products regulated under the Securities and Futures Act (Cap. 289) (SFA). MAS' clarification comes in the wake of a recent increase in the number of initial coin (or token) offerings (ICOs) in Singapore as a means of raising funds.

2 A digital token is a cryptographically-secured representation of a token-holder's rights to receive a benefit or to perform specified functions. A virtual currency is one particular type of digital token, which typically functions as a medium of exchange, a unit of account or a store of value.

3 ICOs are vulnerable to money laundering and terrorist financing (ML/TF) risks due to the anonymous nature of the transactions, and the ease with which large sums of monies may be raised in a short period of time. MAS' media release of 13 March 2014 had communicated that while virtual currencies per se were not regulated, intermediaries in virtual currencies would be regulated for ML/TF risks. MAS is currently assessing how to regulate ML/TF risks associated with activities involving digital tokens that do not function solely as virtual currencies.

4 MAS' position of not regulating virtual currencies is similar to that of most jurisdictions. However, MAS has observed

ICOが匿名で、巨額の資金を短時間に取引できることに起因するマネロン・テロ資金リスク(ML/TFリスク)に着目し、デジタル・トークンの規制を検討していることを公開。

中国の通貨当局はICOを全面禁止



[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

中国はなぜ、ICOと仮想通貨を禁止したのか

Forbes^{JAPAN} 2017/09/24 09:00

「仮想通貨を規制する中国、何が起きているのか」より

- 仮想通貨NEOの運営会社の共同創業者

「中国では週に10件ほどのICOが実施されていた。だが、多く的人是はビットコインを理解していない。ビットコインが何かは分からないが、ただそれで大もうけをしたいと考えていた。...高齢の女性たちが老後の蓄えを投資し始めたことから、政府は介入することにした。」

- 仮想通貨Qtumの運営会社の共同創業者

「ICOが人気を得るようになるにつれて、多くの人当初の目的を忘れ始めていたようだ。詐欺と見られるICOプロジェクトもあった。だが、中国人たちは詐欺かどうかを見分けることができない。ICOを理解していないのだ。中国にはICOプラットフォームが65あり、これらの数が増えたことで簡単に投資ができるようになったことも、こうした状況を加速させていた。」

中国はビットコイン交換所もマイナーも規制



ビットコイン、中国での「採掘」に終止符 当局が停止命令

中国当局はビットコイン採掘活動の停止を命じた。同国では規制によって既にビットコイン取引所が閉鎖されたが、さらに世界のビットコイン供給の大きな部分を...

JP.WSJ.COM

韓国も規制強化の方針と伝えられた



韓国、仮想通貨の取引を禁止する法案を準備中＝法相

【ソウル 11日 ロイター】 - 韓国の朴相基（パク・サンギ）法相は11日、仮想通貨の取引所取引を禁止する法案を法務省が準備していることを明らかにした。

麻生大臣の発言に注目が集まる

麻生金融相、仮想通貨「何でも規制すればいいとは思わない」

経済・政治

2018/1/12 10:08

 保存  共有  印刷     その他▼

麻生太郎財務・金融相は12日午前の閣議後の記者会見で、価格の乱高下が続くビットコインなどの仮想通貨に関し「何でもかんでも規制すればいいとは思わない」と語った。「利用者保護とイノベーションのバランスを注意しながらやっていかなければいけない」と述べ、当面は状況を見極める姿勢を示した。

中国や韓国など一部の国で規制強化の動きがあることについて「他国のことに関してはどうのこうのというつもりはない」と説明した。そのうえで「仮想通貨がどうなっていくかはまだ意見の分かれるところだ。我々としては市場がどういったものに大きく化けていくのか、（既存の）通貨に代わる制度かどうかはまだ見えてきていない」と語った。〔日経QUICKニュース（NQN）〕

フランスとドイツは3月のG20で 仮想通貨の国際的な規制を提案する方針

G20、仮想通貨規制を議論 仏独提案へ

経済

2018/1/19 12:46

🔖 保存 📧 共有 🖨 印刷 🌐 共有 COME 🐦 f その他▼

ロイター通信によると、フランスとドイツは3月にアルゼンチンで開かれる20カ国・地域（G20）財務相・中央銀行総裁会議で、仮想通貨の国際的な規制を呼びかける方針だ。フランスのルメール経済・財務相は18日、「ビットコインのリスクの分析や規制についてドイツとともにG20参加国に提案したい」と述べた。両国がパリでの共同記者会見で発言した。

ルメール氏は仮想通貨の値動きの激しさが金融システムに引き起こしうるショックや、マネーロンダリング（資金洗浄）への悪用を懸念しているとみられる。仮想通貨相場はこのところ下落が目立つ。代表的なビットコインの価格は1月中旬に入って2017年12月中旬につけた最高値のほぼ半値にまで落ちた。

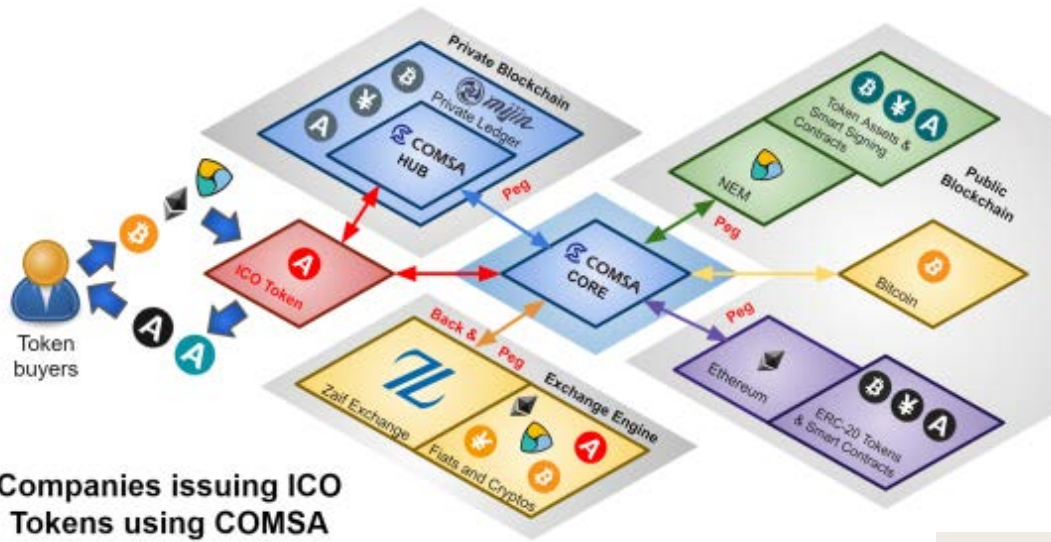


🔍 画像の拡大

ビットコインの規制について議論する

ドイツのアルトマイヤー財務相代行も「我々は市民に対してリスクを説明し、規制によってリスクを低減させる責任を負っている」と述べた。

日本ではICOプラットフォームの新規構築が進む



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。

6. Blockchain 2.0とthe DAO事件

Blockchain 2.0

近年、「ブロックチェーン2.0」と呼ばれる新たなサービスが勃興している。

- bitcoinのような仮想通貨としてのブロックチェーンを1.0とした時に、「契約」の機能を果たすものを2.0と位置付ける呼称。

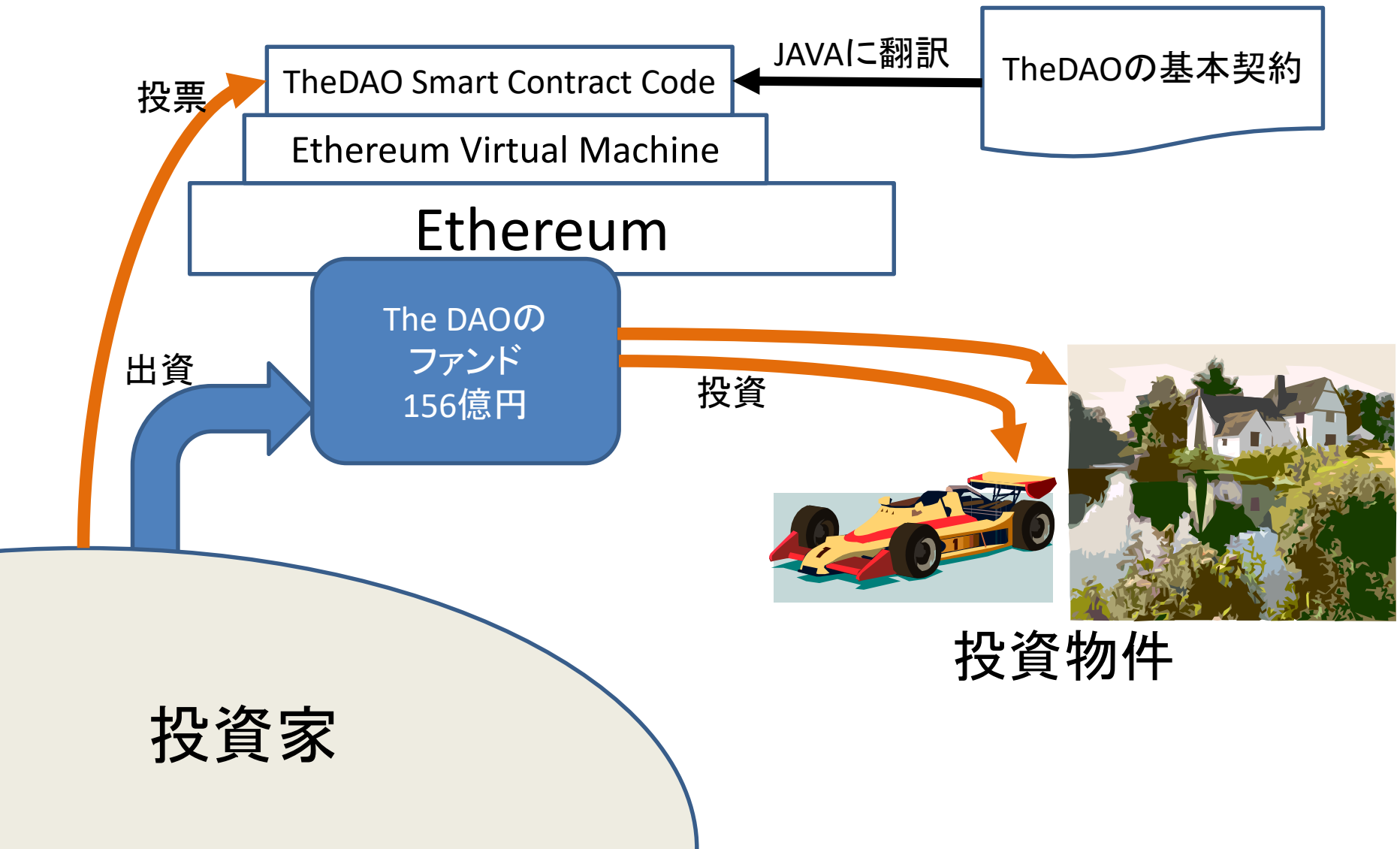
スマートコントラクト	契約書をブロックチェーンに載せ、契約を執行させる機能を持たせたもの。
スマートプロパティ	資産・契約書をブロックチェーンに載せたもので、契約を執行させる機能はない。
DAO (Decentralized Autonomous Organization)	分散型自動化組織。スマートコントラクトをさらにまとめて、自動執行するようにしたもの。
DAC (Decentralized Autonomous Corporation)	DAOの会社版。出資をして株主のために配当を支払うこと等を自動的にブロックチェーン上で行う。

その一類型として、“DAO”がある（一般名詞としてのDAO）。

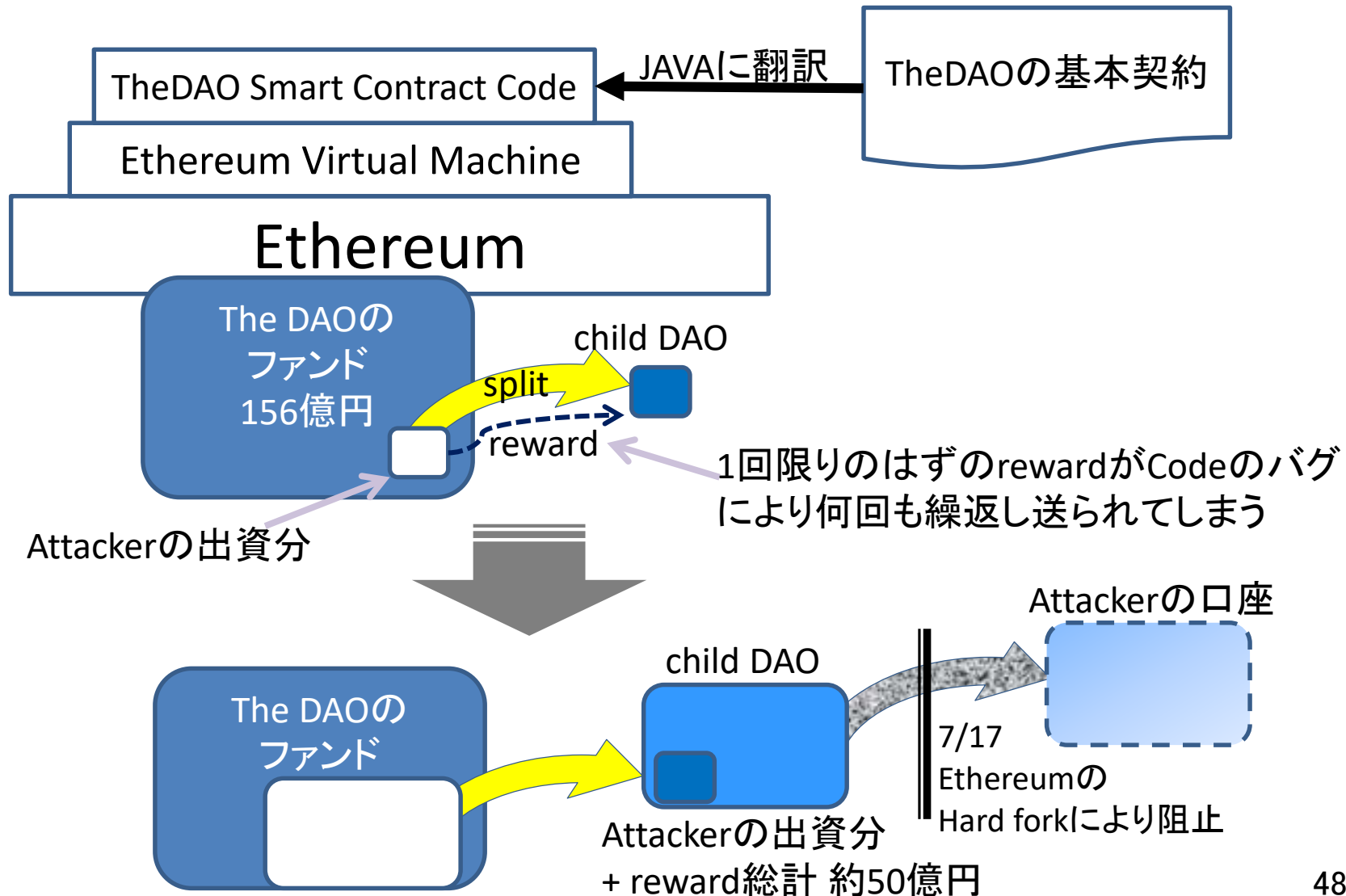
The DAOとは

- The DAO(固有名詞)は、ドイツのIoTベンチャー企業であるSlock.it社が、DAO(一般名詞)のコンセプトを実証するために2016年4月30日にEthereum上に組成した事業ファンド。組織を運営する役員を置かず、Ethereum上で出資したメンバーが投票によってガバナンスする仕組み。
- Slock.it社は、IoTを活用したシェアリング・エコノミーの展開を目指しており、スマートロック(IoT接続された電子的な錠)が装備された車、家などを、Ethereum決済によって利用可能とする事業を展開。その一部は、AirB&Bでも活用されている。
- The DAO は2016年5月に出資を募り、5月28日までに11000人の投資家から約156億円を調達した。

The DAOの基本構造



The DAO事件：攻撃の手口



7. 中央銀行デジタル通貨を巡って

デジタル通貨発行「具体的計画ない」、不断に研究＝黒田日銀総裁

Reuters

2017/10/04



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。

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、渡邊明彦、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・ペイメント・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、中央銀行発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は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、实体经济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。

BIS Quarterly Review (2017年9月)掲載CBCC論文

Morten Bech
morten.bech@bis.org

Rodney Garratt
garratt@ucsb.edu

Central bank cryptocurrencies¹

New cryptocurrencies are emerging almost daily, and many interested parties are wondering whether central banks should issue their own versions. But what might central bank cryptocurrencies (CBCCs) look like and would they be useful? This feature provides a taxonomy of money that identifies two types of CBCC – retail and wholesale – and differentiates them from other forms of central bank money such as cash and reserves. It discusses the different characteristics of CBCCs and compares them with existing payment options.

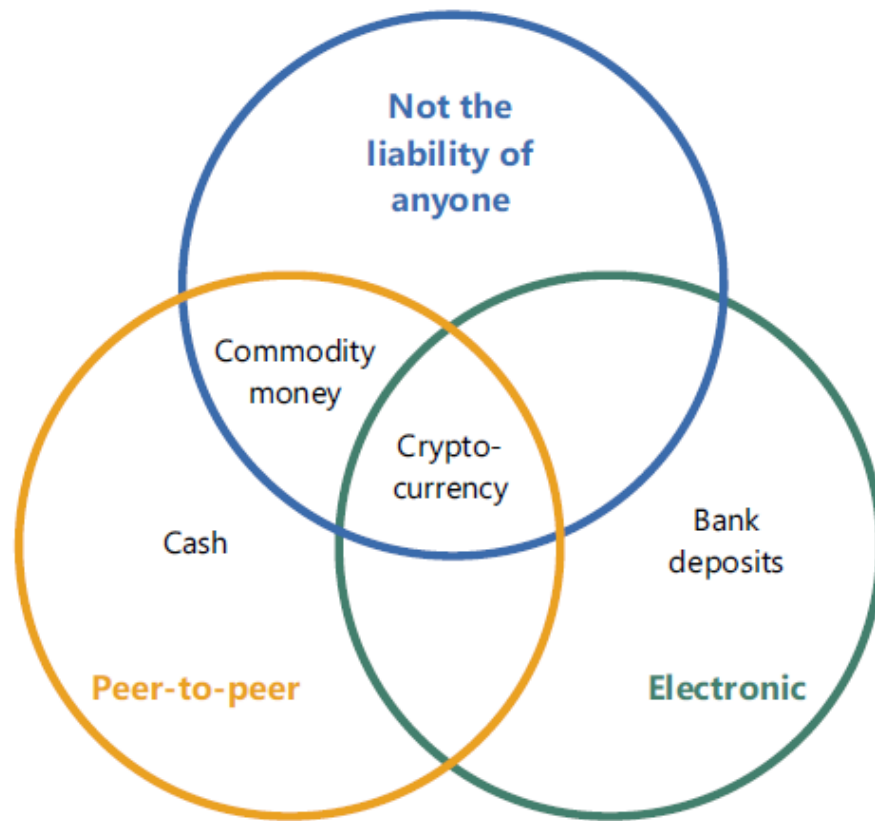
JEL classification: E41, E42, E51, E58.

従来の2つの分類法

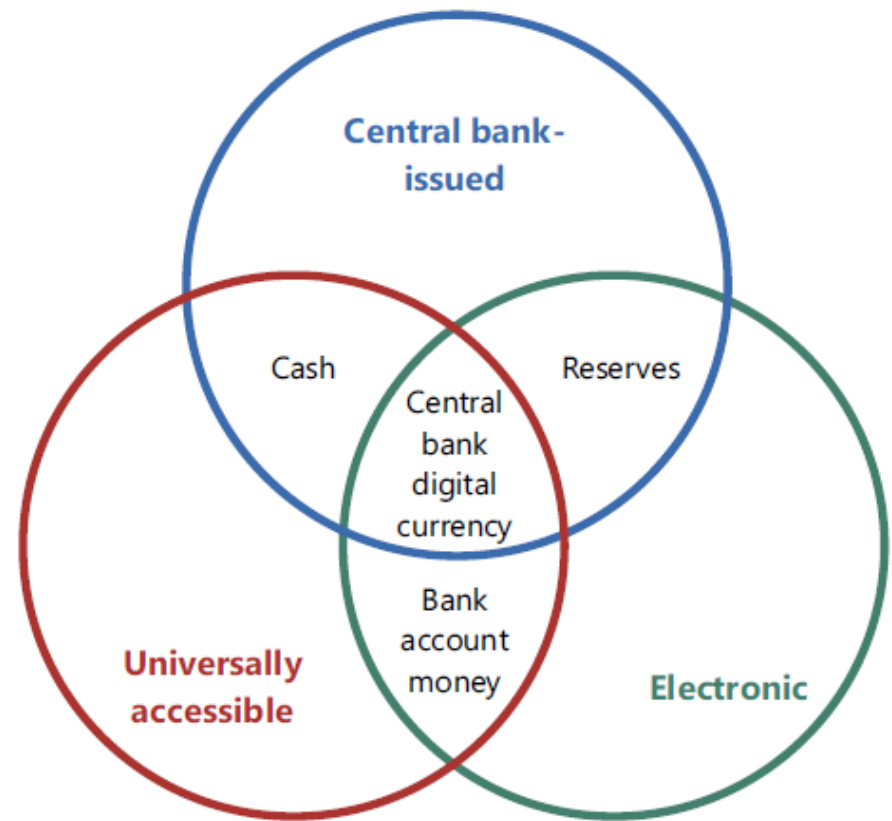
Two taxonomies of new forms of currency

Graph 2

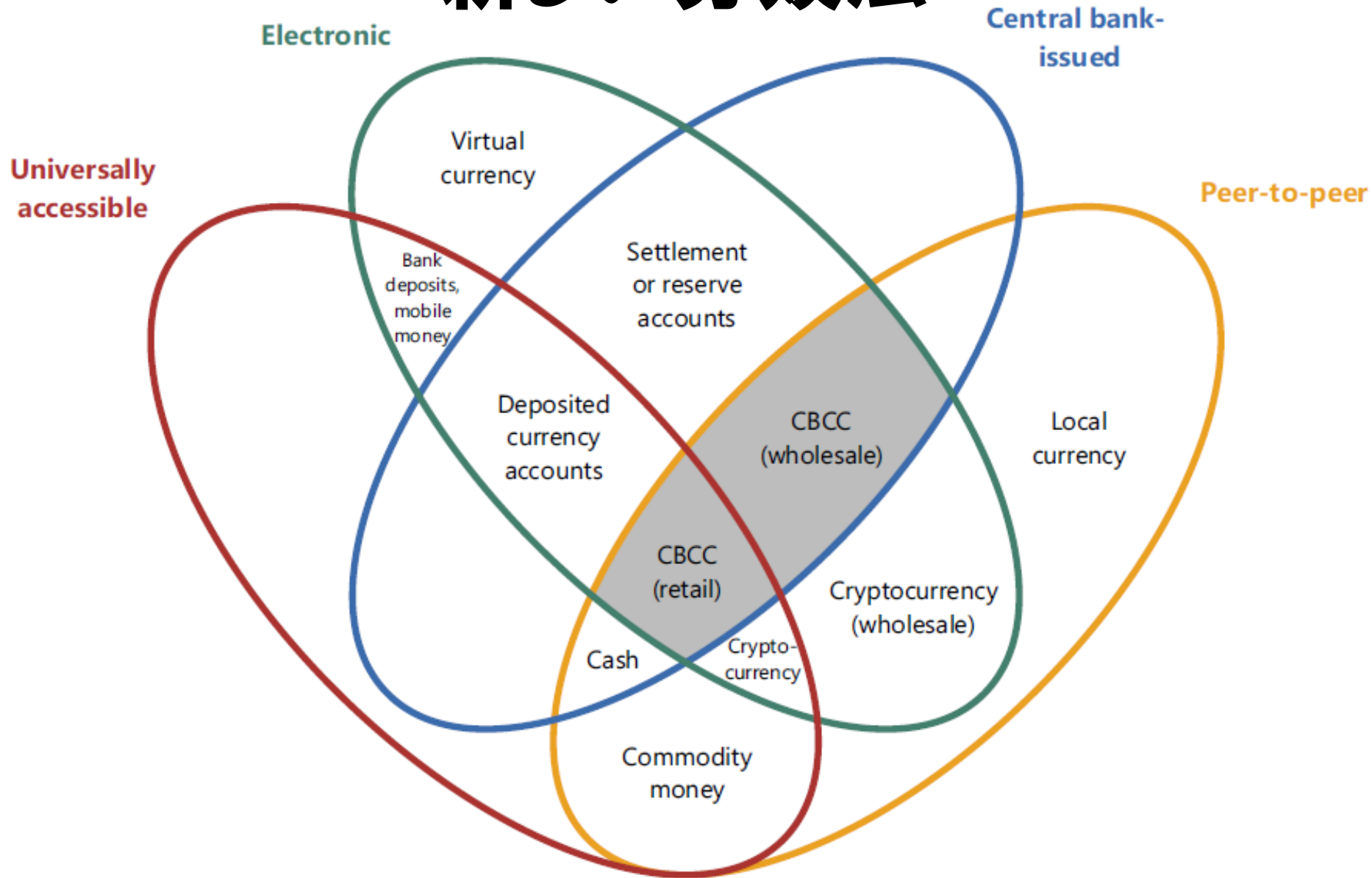
Cryptocurrency, CPMI (2015)



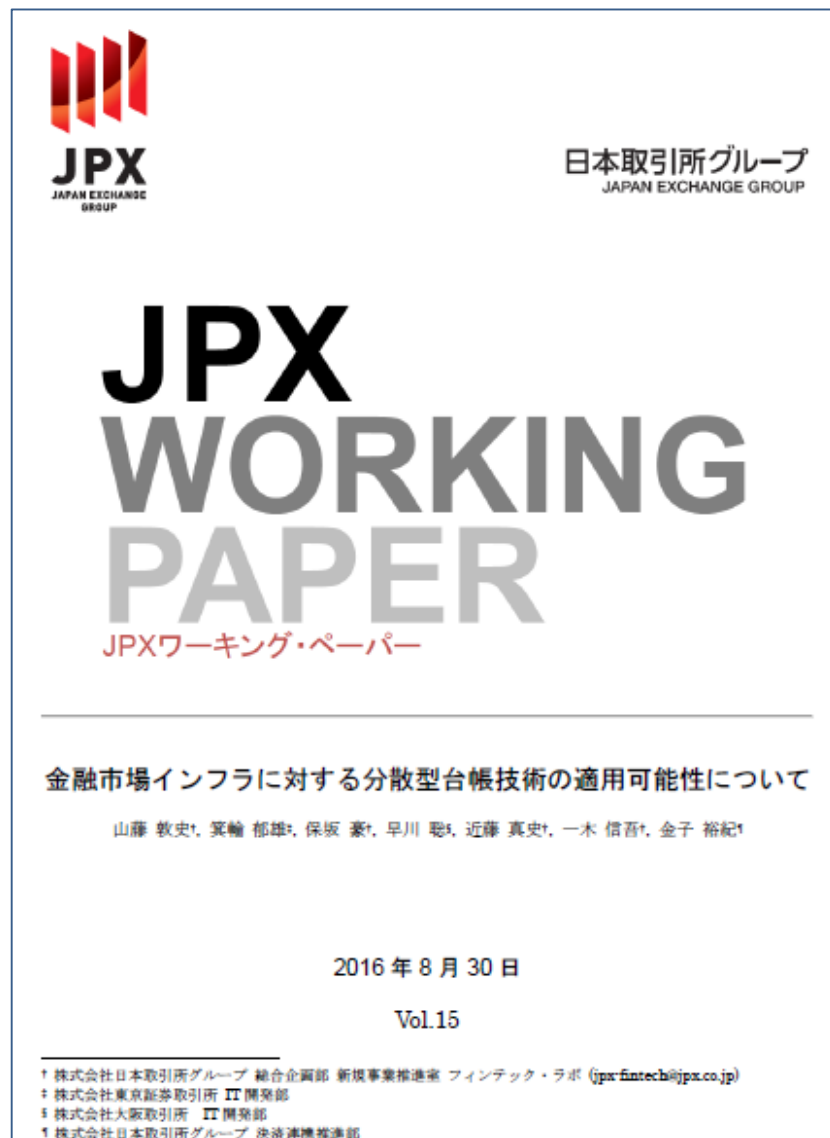
Central bank digital currency, Bjerg (2017)



新しい分類法

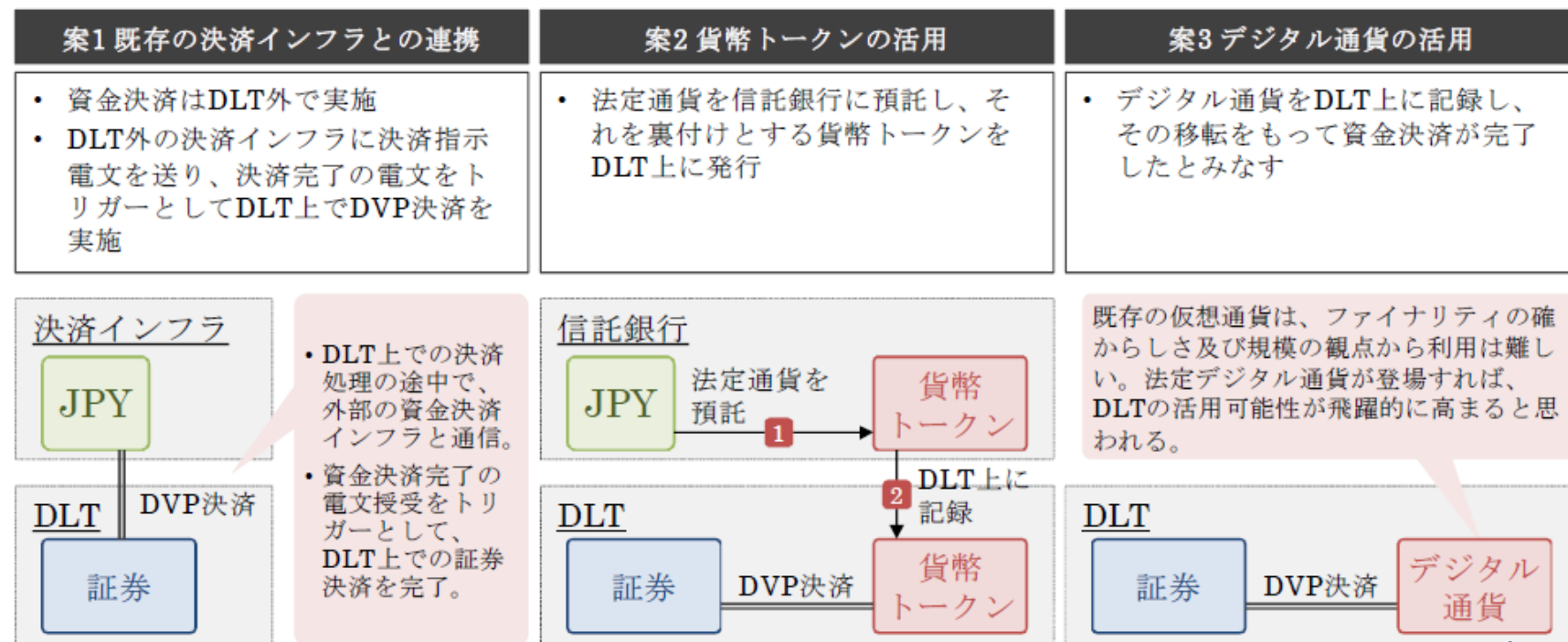


日本取引所の分散型台帳WPから



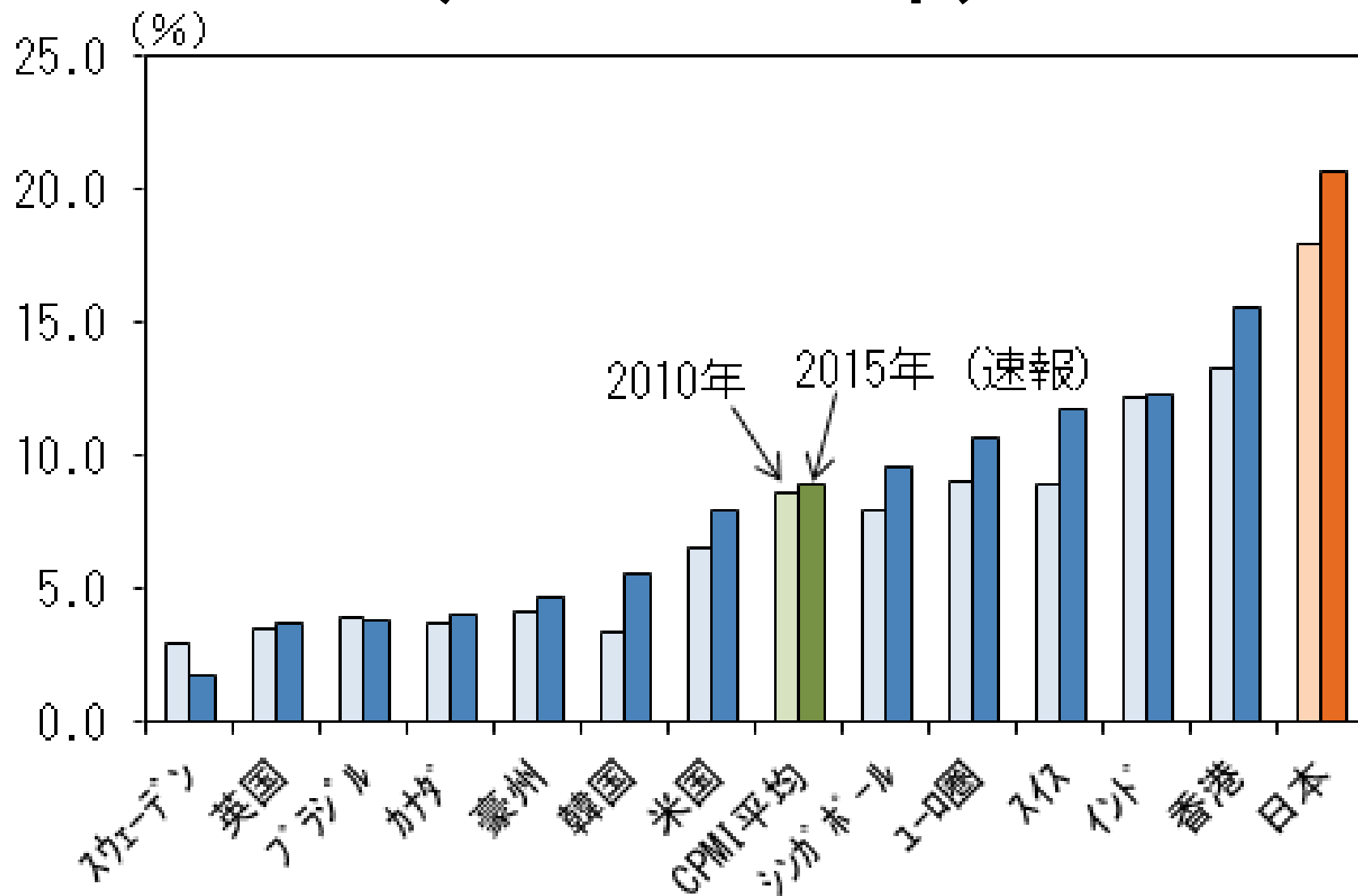
証券決済DVP実現の対応案

図 9 DLT 上で資金決済を行う対応案



安定したファイナリティと十分な発行量を保証する法定デジタル通貨を中央銀行が発行し、DLT上で取り扱う事を可能とすれば、これらの問題を抜本的に解決する可能性がある。⇒ CBCC(wholesale)

主要国における対GDP通貨流通残高比率の推移 (2010→2015年)



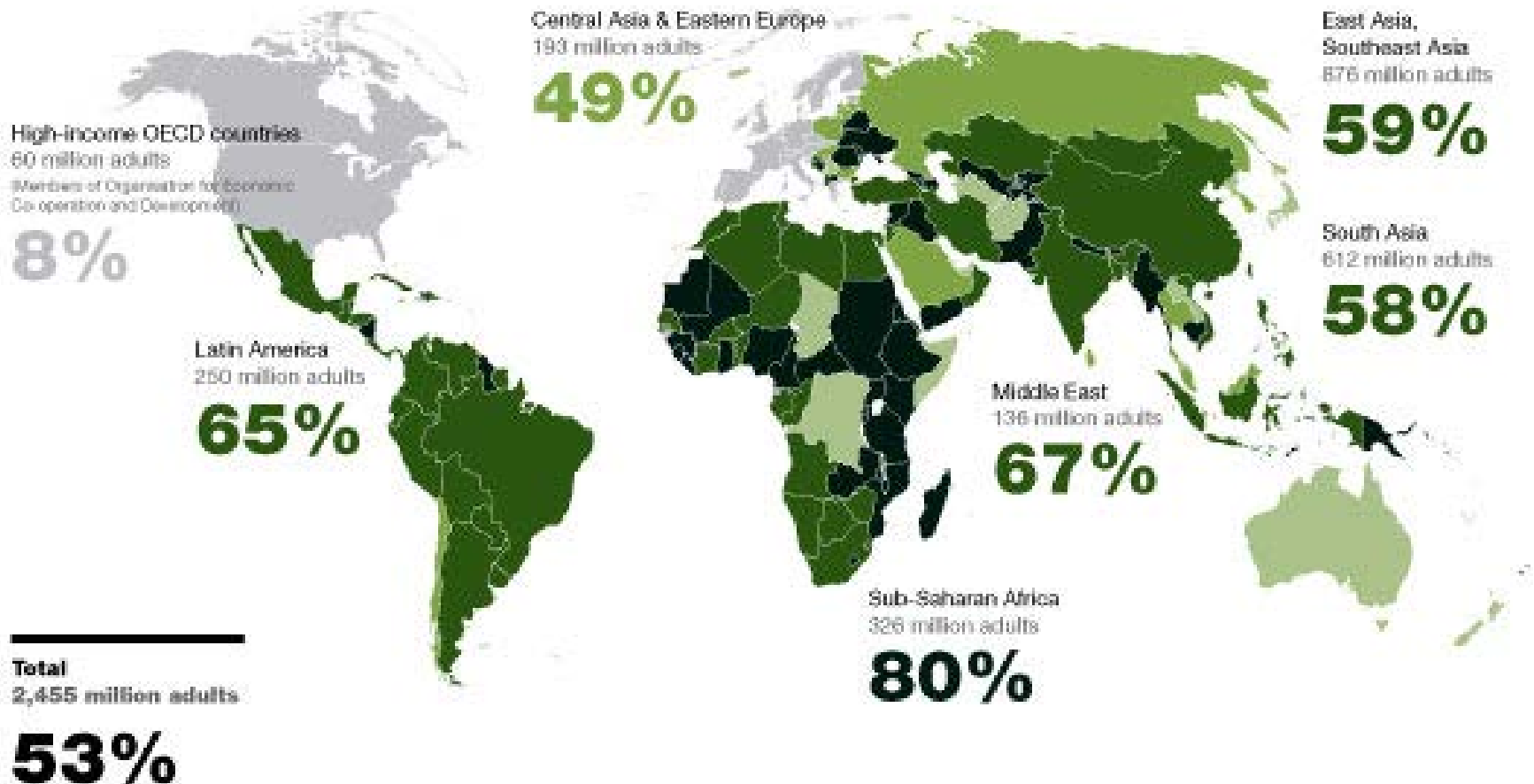
(出所) 国際決済銀行 決済・市場インフラ委員会

世界人口の約半分は銀行が使えない

Percentage of total adult population who do not use formal or semiformal financial services

0-25% 26-50% 51-75% 76-100%

Estimates used to calculate regional averages



M-PESAが金融包摂を実現した



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-PESAで、銀行の支店がなく、現金を持ち歩くことAによっても危険なケニアの地方で

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・マトラウ(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

ITU-T デジタル法定通貨検討グループ

ITU-T(International Telecommunication Union - Telecommunication Standardization Sector) は、国際電気通信連合の部門の一つで、通信分野の標準策定を担当する電気通信標準化部門)の検討グループとして、Focus Group on Digital Currency including Digital Fiat Currency (FG DFC)が2017年に設立された。議長団には、アフリカ諸国に加え、中国、ロシア、インドが参加している。

Chairman: David Wen, eCurrency

Vice Chairmen:

Yao Qian, Institute of Digital Money, People's Bank of China

Yury Grin, Intervale, Russia

Ahmed Said, NTRA, Egypt

Mandar Deshpande, Ministry of Communications, India

Njunga N'dungu, University of Nairobi, Kenya

Workshop on Standards for Digital Fiat Currency (DFC) for Universal Financial Access

12 October 2017

09:30 – 10:30	Keynote Address • Basic Components of Digital Fiat Currency – Mr Yao Qian, Institute of Digital Money, the People's Bank of China
10:45 – 12:00	SESSION 1: Policy and Regulatory Landscape
12:00 – 13:15	SESSION 2: Regional Spotlight: The Chinese Experience for Digital Financial Access
14:15 – 15:30	SESSION 3: DFC Application in Developed and Developing Economy
15:45 – 17:00	SESSION 4: Security Issues in Digital Financial Services
17:00 – 18:15	SESSION 5: Architecture of DFC for Interoperability

Bilel Jamoussi, chief of the Study Groups Department at the ITU Standardization Bureau, praised the presentation of Yao Qian, director-general of the Institute of Digital Money at the PBOC, and said the workshop was impressive.

In Yao's speech, he noted the PBOC has completed trial runs on the algorithms needed for digital currency supply and has designed a prototype that can regulate the supply.

南米におけるデジタル通貨の実装

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。



最初の実装：エクアドル

最初に中央銀行デジタル通貨が発行された国は、エクアドルである。2014年12月、エクアドルは中央銀行発行の電子通貨「ディネロ・エレクトロニコ(EI dinero electrónico)」を導入した。

2000年、エクアドルは長年続いたインフレに対処するために、独自通貨を発行するのをあきらめ、「ドル化(dollarization)」に踏み切ることを決断した。エクアドルの国内では、自国通貨が信頼を失い、米国から輸入されたドルの現金が決済手段として使われた。

この荒療治によって、インフレは沈静化したが、政府は古いドル紙幣を新しいものと交換するために、毎年300万ドルの経費がかかった。政権交代を契機に、中央銀行が新たに電子通貨を発行することとしたのだ。

しかし、独自電子通貨が折角鎮静化させたインフレを再燃させてしまっては元も子もない。このため、ディネロ・エレクトロニコは、「携帯電話で使える低所得者向けのデビットカード的な決済手段」として導入されたのだ。今のところ、ドル化した金融システムはそのまま、その外縁を支えるサブシステムとして、一部の低所得者向けの独自電子通貨が発行されたに過ぎない。将来的にはその領域を拡大することを目標に、実証実験的な意味合いで導入されたものと言われている。

第二の実装：ウルグアイ

2017年11月、ウルグアイでも中央銀行がデジタル通貨を発行した。1万人を対象に、通貨ペソと同価値の法定デジタル通貨「eペソ」2000万ペソ(約7800万円)分を発行した。

ウルグアイも、1%台の低成長、8%台の高インフレという経済の構造問題を抱えている。こうした既存の通貨システムに問題を抱える国であれば、そうしたチャレンジに走りやすい傾向がある。

第三の実装は実現するか：ベネズエラ

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中央銀行デジタル通貨（暗号通貨とも報じられる）「ペトロス（Petros）」の最初の1億ペトロス分の発行を命じた。同大統領によれば、1ペトロスは1バーレルのベネズ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、「Petro」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ふ。

ペトロス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、流通するとされ、そのための発掘業者向けの説明会が予定されているという。現時点では、この構想がどの程度の技術体系に基づいて設計されたものか、その価値と石油の価値とを紐づけるとは具体的にどういうことなのかなど、不明なことが多い。

ベネズエラは、長年続いた反米主義のチャペス大統領の没後、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、中央銀行デジタル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。

ところが、、、

ベネズエラPetroをめぐる争い

2018年1月10日、ベネズエラの「石油担保公定暗号通貨」Petroに関する大統領令が国会で違法と判断された。今回の議会の決定で、大統領令は失効すると報じられているが、大統領は発行を決行する方針のようだ。



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



22 hours ago | Kevin Helms | 11779 | 57

Venezuela Will Pre-Mine Its Cryptocurrency Petro and Launch in 6 Weeks

Bitcoin.com