PKI Day 2018　　2018年4月17日

トラストとトラストレスの狭間で

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

1. 仮想通貨取引の実際

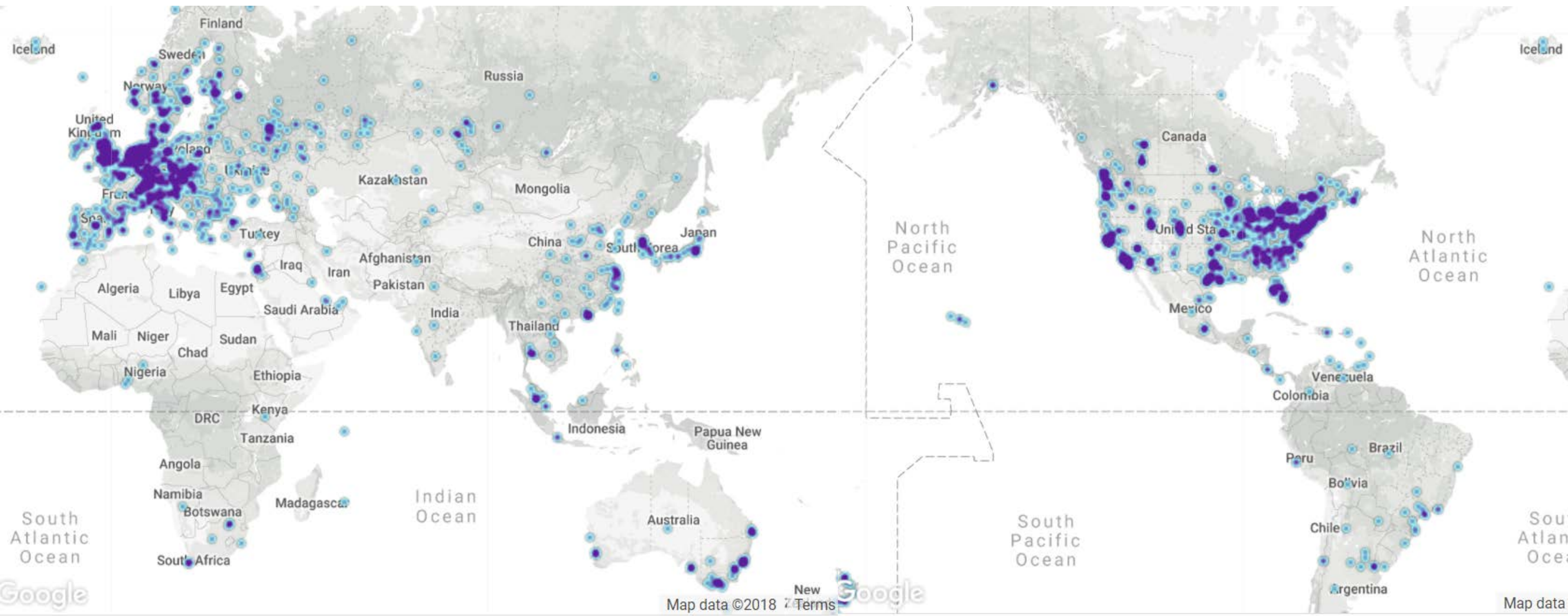
GLOBAL BITCOIN NODES DISTRIBUTION

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)



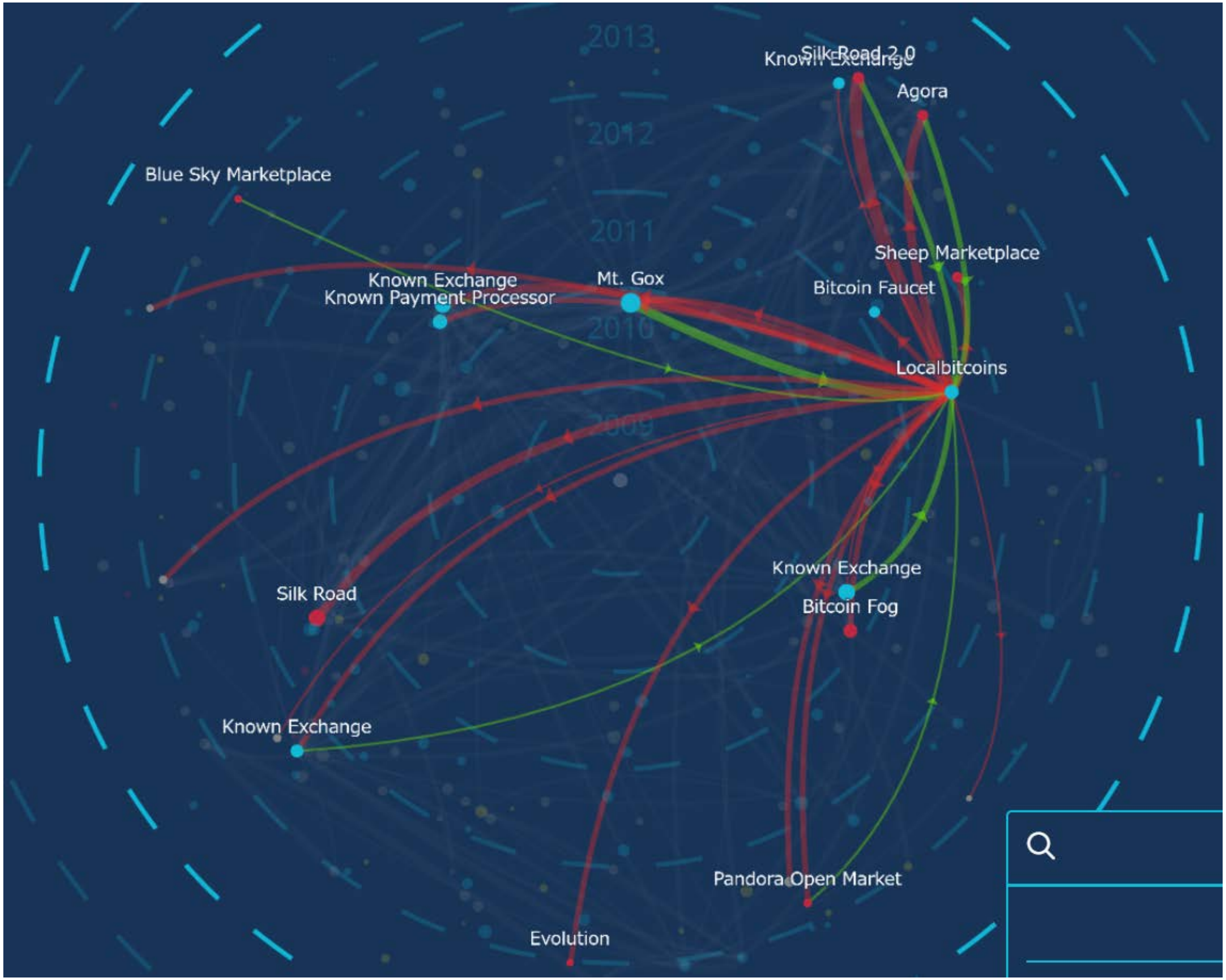
ap shows concentration of reachable Bitcoin nodes found in countries around the world.

ap shows concentration of reachable Bitcoin nodes found in countries around the world.

(source) bitnodes.earn.com/

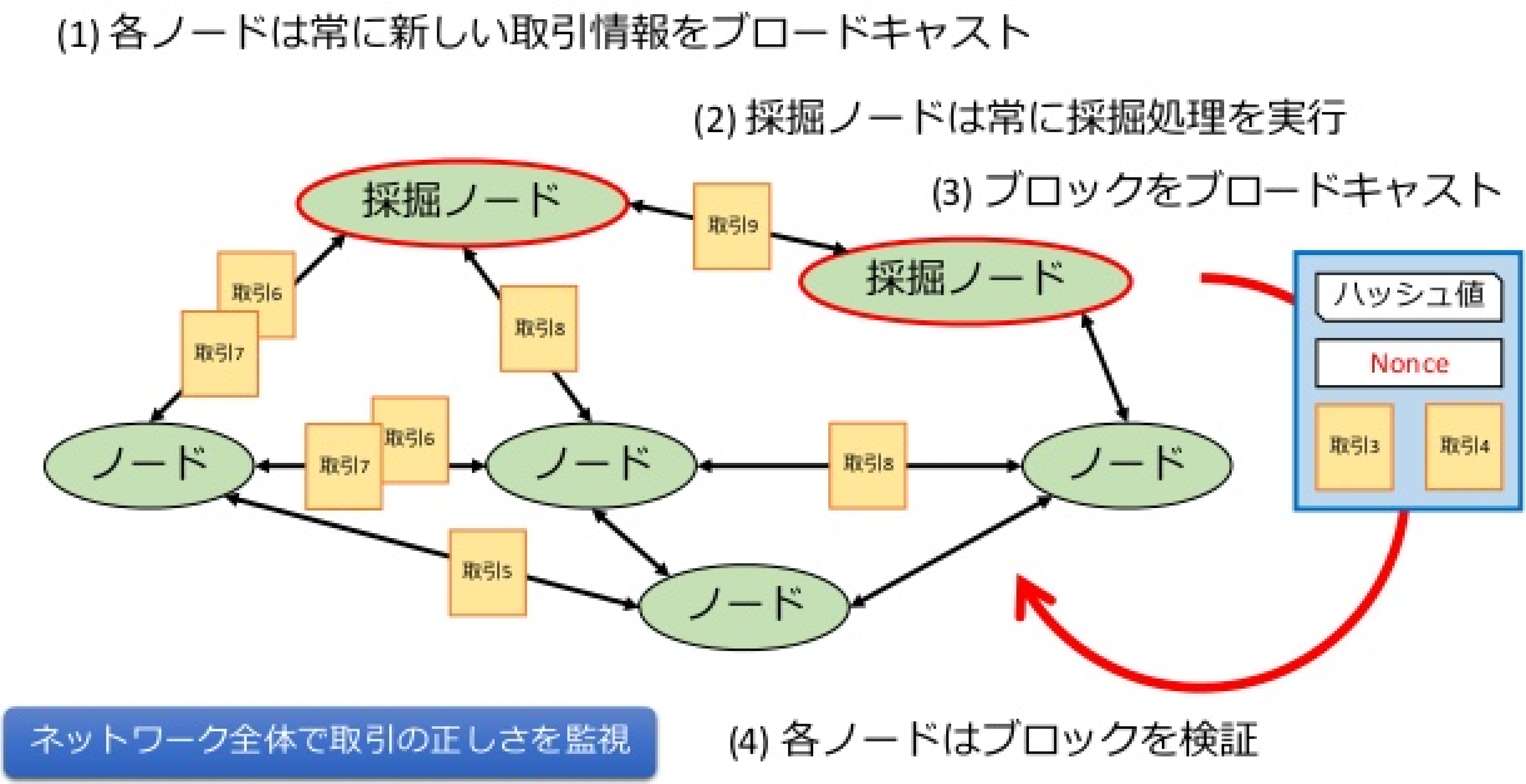
THE BITCOIN BIG BANG

A demonstration of our ability to track transactions through entities on the blockchain; the Big Bang shows the emergence of the largest 250 entities on the blockchain, their identity, and interconnectivity.



（source）www.elliptic.co

ビットコイン採掘時の各ノードの役割



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

Economist

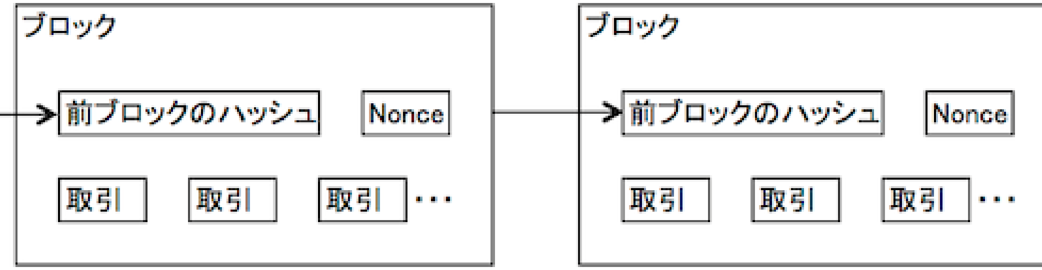
Bitcoinの発掘の仕組み

Bitcoin

The magic of mining

Minting the digital currency has become a big, ru

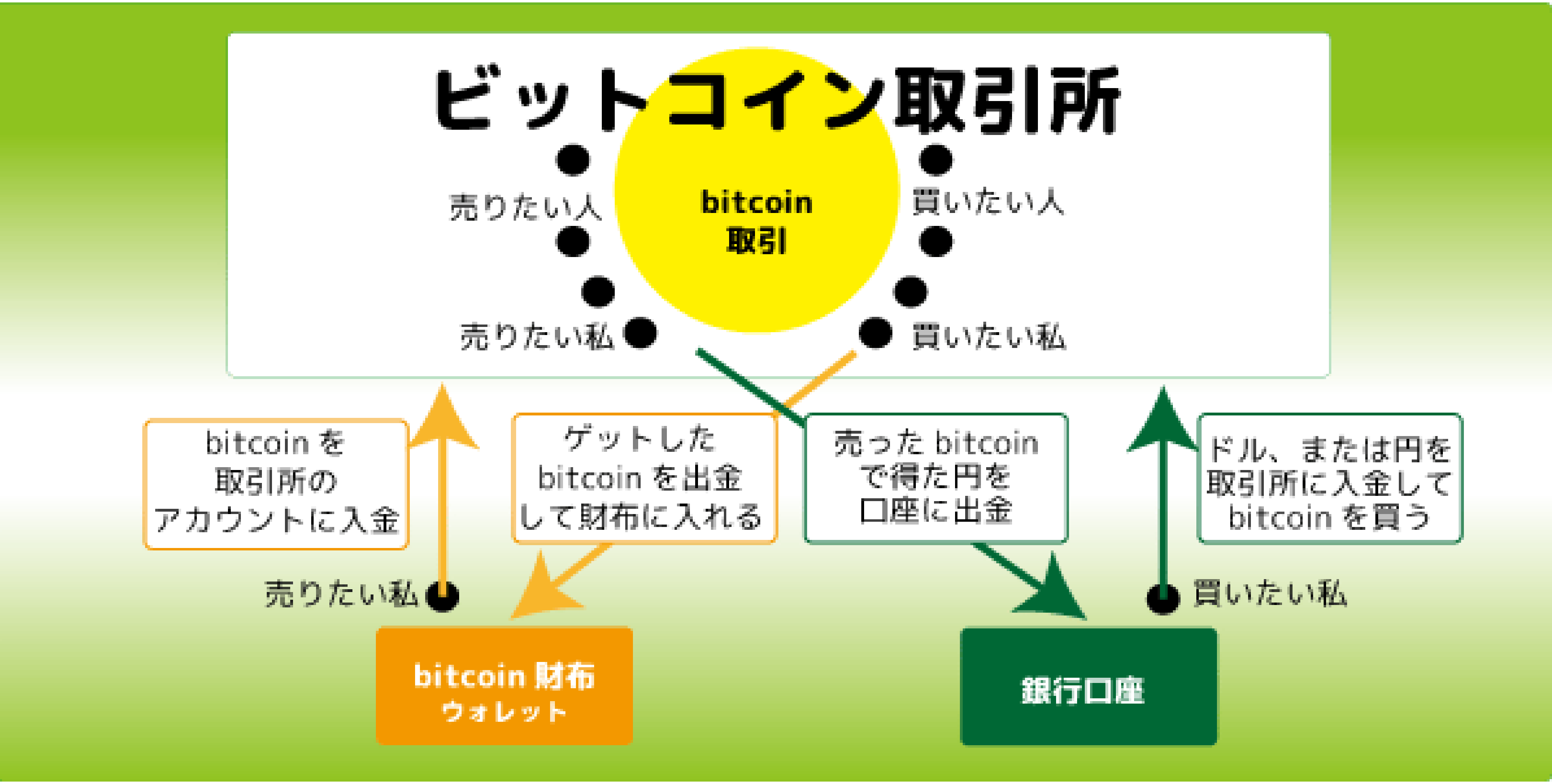
Jan 10th 2015 | BODEN, SWEDEN | From the print edition



Timekeeper

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。

ビットコイン取引所での売買のイメージ



はじめてのビットコイン仮想通貨　https://kuchikomi0.com/virtualmoney/bitcoin/

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。

２. 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.

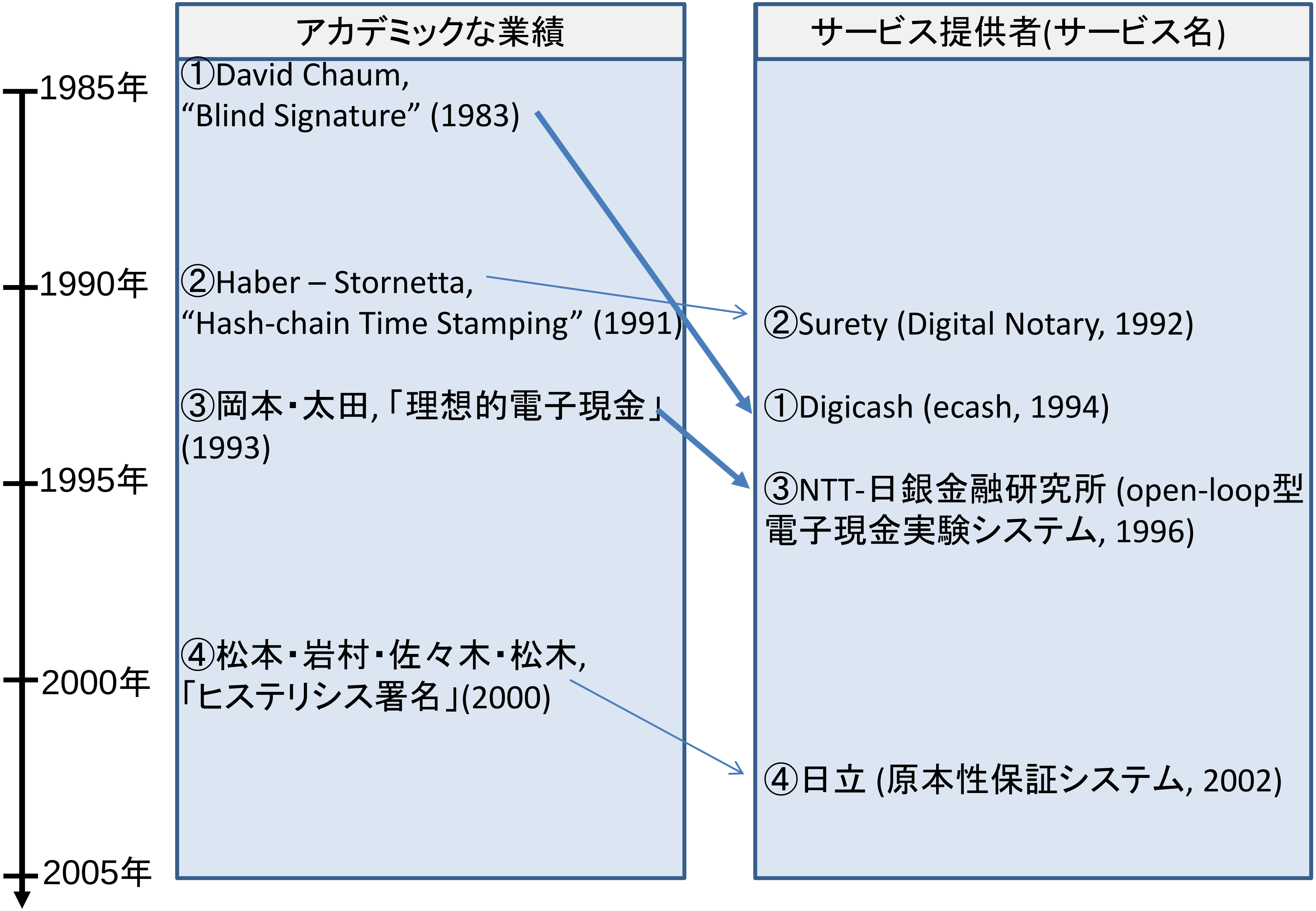
Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

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



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。

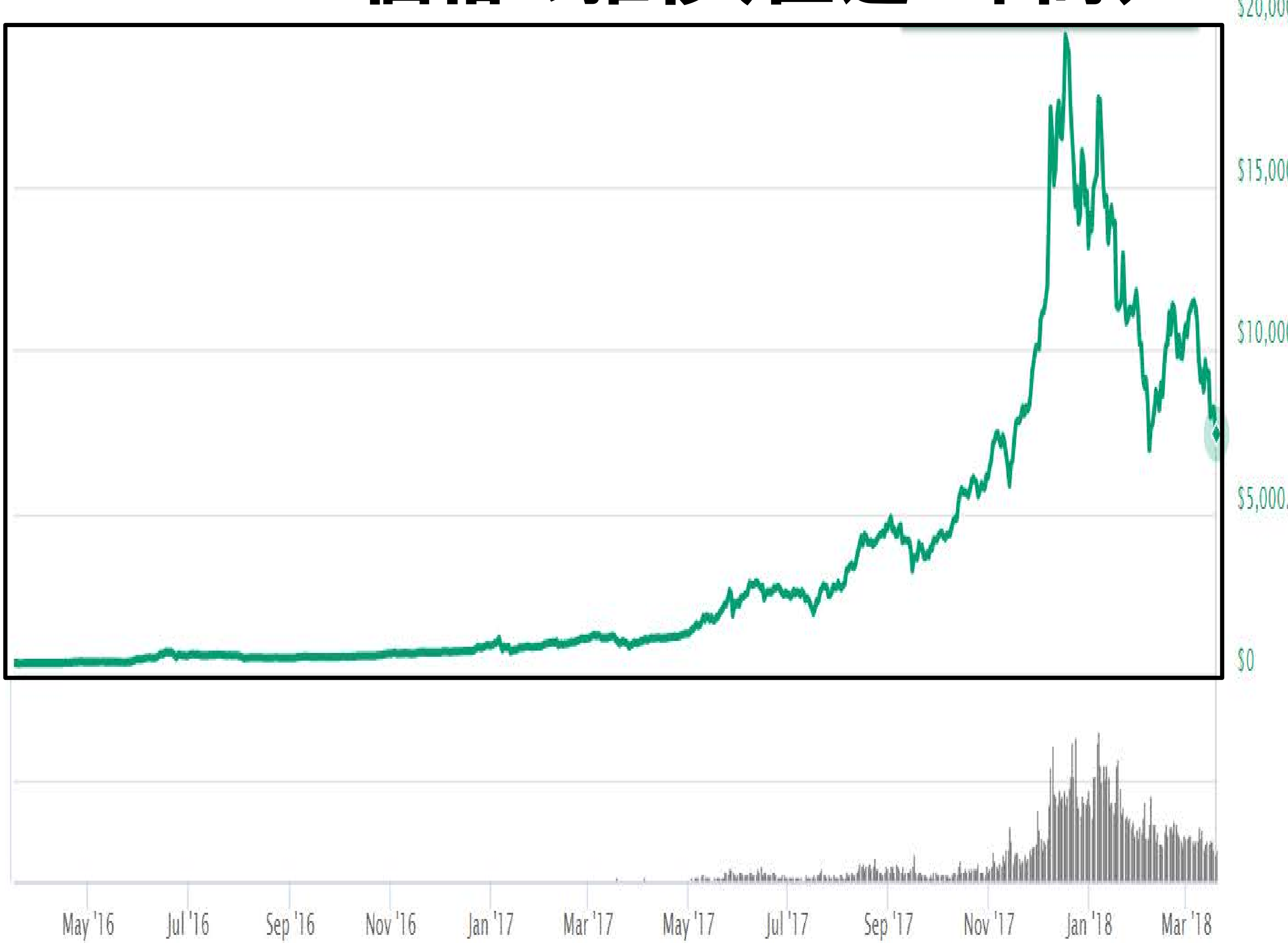
⇒ システム維持費用の「自給自足」が可能な仕組みを構築できたことが、現在の「成功」の一因と考えられる。

３．仮想通貨価格の乱高下とその原因

（1年前の）Bitcoinの価格と利用者数の推移

（出所）blockchain.info

Bitcoin価格の推移（直近2年間）

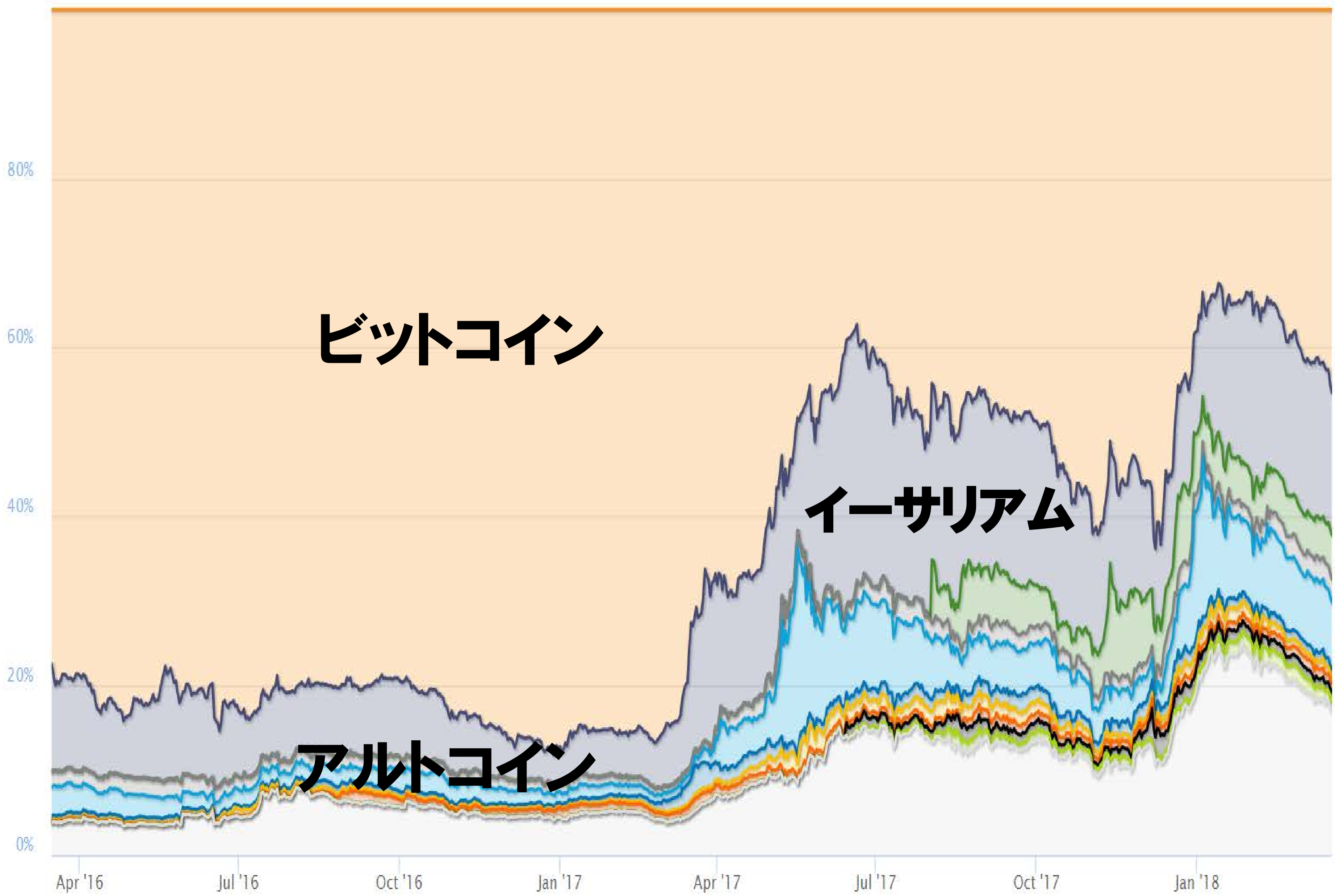


（出所）coinmarketcap.com

全仮想通貨の時価総額の推移（直近2年間）

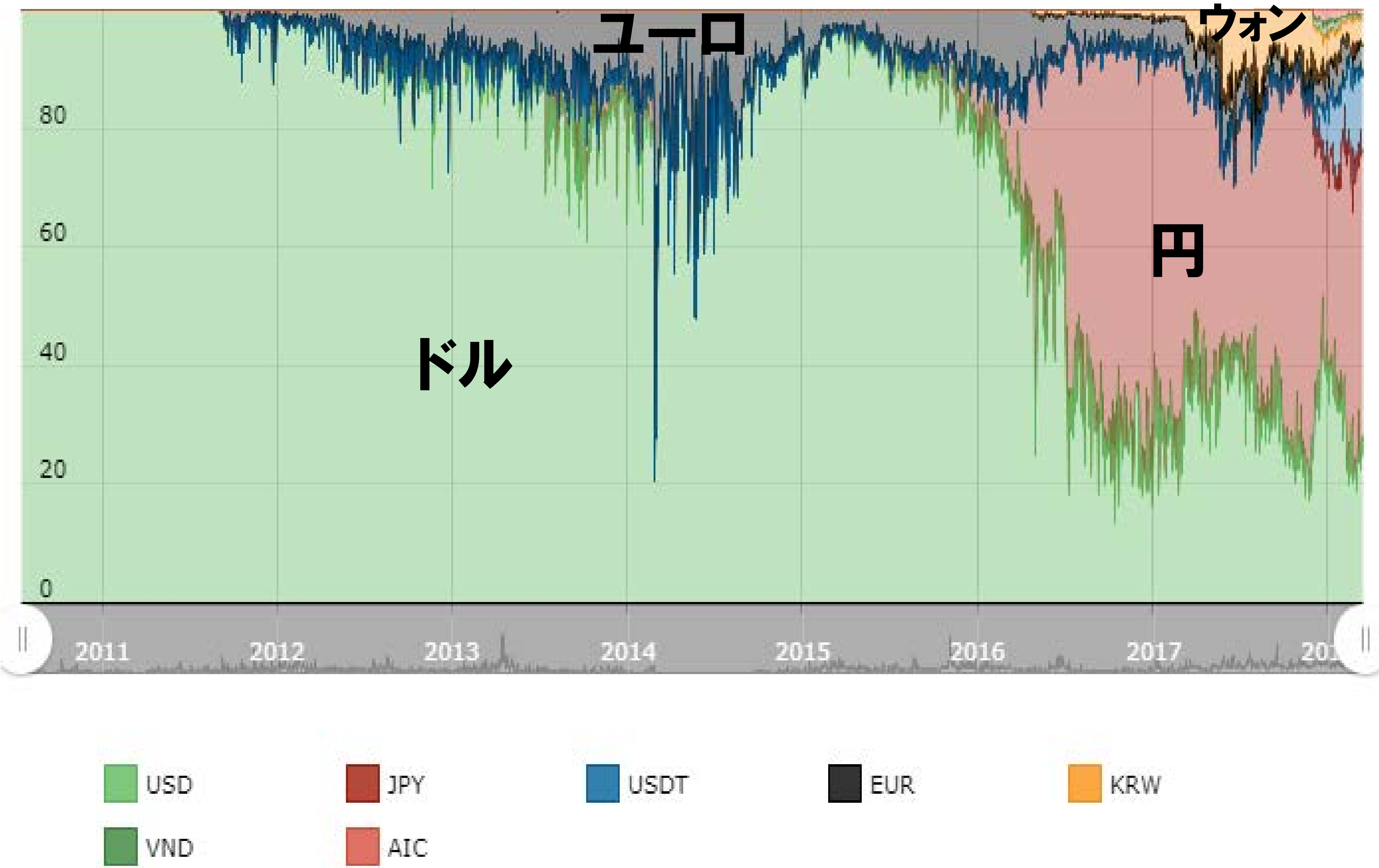
（出所）coinmarketcap.com

仮想通貨の通貨別流通総額の構成比の推移（直近2年間）



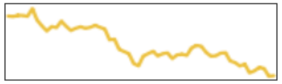
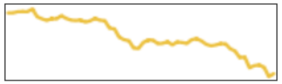
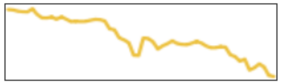
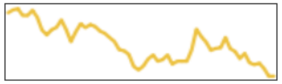
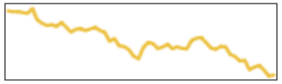
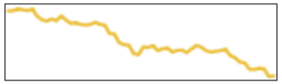
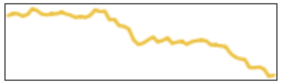
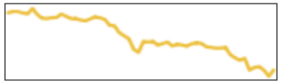
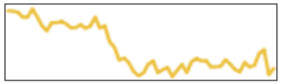
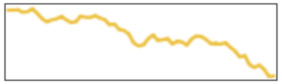
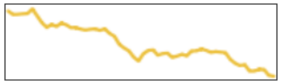
（出所）coinmarketcap.com

Bitcoinの通貨別取引額の構成比



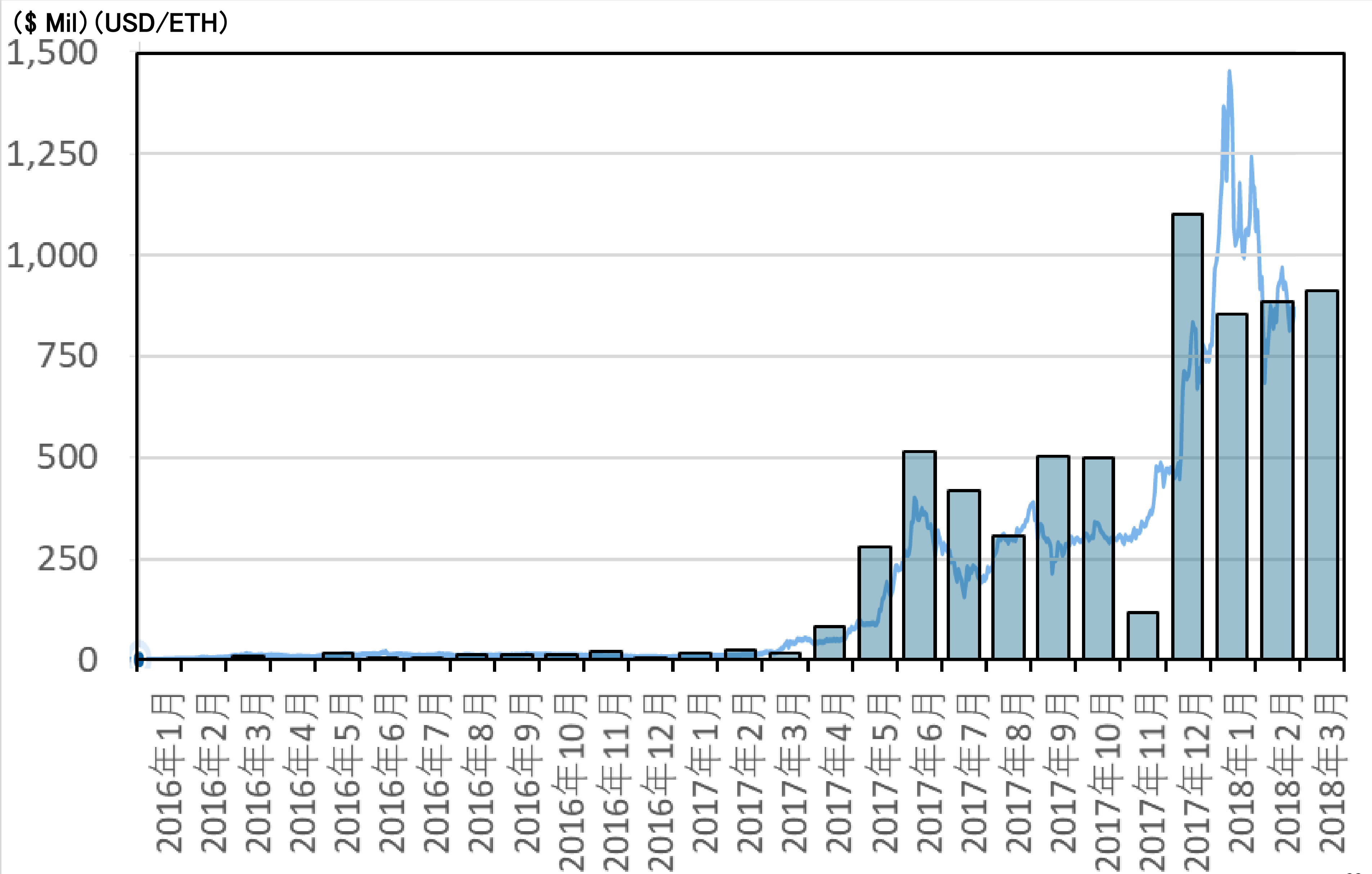
（出所）www.cryptocompare.com

仮想通貨の時価総額上位銘柄

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$127,111,696,766	$7,509.66	$5,344,280,000	16,926,425 BTC	-5.47%	
2	Ethereum	$47,962,413,419	$488.08	$2,134,250,000	98,267,525 ETH	-14.72%	
3	Ripple	$22,264,882,600	$0.569555	$601,581,000	39,091,716,516 XRP *	-11.66%	
4	Bitcoin Cash	$14,781,694,285	$868.25	$390,972,000	17,024,738 BCH	-9.83%	
5	Litecoin	$7,926,053,258	$142.34	$492,809,000	55,684,731 LTC	-8.19%	
6	NEO	$3,504,104,500	$53.91	$156,246,000	65,000,000 NEO *	-15.64%	
7	Cardano	$3,426,677,205	$0.132166	$125,370,000	25,927,070,538 ADA *	-16.59%	
8	Stellar	$3,380,967,611	$0.182768	$68,150,200	18,498,684,731 XLM *	-11.97%	
9	IOTA	$3,101,566,662	$1.12	$93,363,200	2,779,530,283 MIOTA *	2.14%	
10	EOS	$3,021,952,024	$4.10	$252,358,000	736,518,960 EOS *	-14.43%	
11	Monero	$2,876,550,131	$181.62	$54,841,400	15,838,202 XMR	-8.75%	
12	Dash	$2,804,391,559	$352.59	$108,387,000	7,953,713 DASH	-10.02%	

（出所）coinmarketcap.com

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

４．ICOを巡る国内外の動き

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トークンの価格と収益率(3月11日→19日の変化)

Name	USD Raised	Month	Token Sale Price	2018-03-11 トークン価格	2018-03-11 収益率	2018-03-19 トークン価格	2018-03-19 収益率
Sirin Labs	$157,885,825.00	Dec 2017	$0.470	$0.590	1.26x	$0.352	0.75x
The Bancor Protocol	$153,000,000.00	Jun 2017	$3.857	$3.847	1.00x	$2.548	0.66x
QASH	$108,174,500.00	Nov 2017	$0.309	$0.648	2.10x	$0.430	1.39x
Status	$107,664,904.20	Jun 2017	$0.036	$0.135	3.77x	$0.078	2.17x
Envion	$100,012,279.00	Jan 2018	$0.803	$0.592	0.74x	$0.515	0.64x
Kin	$98,500,326.08	Sep 2017	$0.000	$0.000	2.27x	$0.000	1.52x
COMSA	$95,614,242.43	Nov 2017	$1.000	$0.664	0.66x	$0.487	0.49x
TenX	$83,110,818.40	Jun 2017	$0.805	$1.277	1.59x	$1.001	1.24x
Elastos	$70,644,600.00	Jan 2018	$8.920	$47.386	5.31x	$30.549	3.42x

(出典) https://www.tokendata.io/advanced

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。

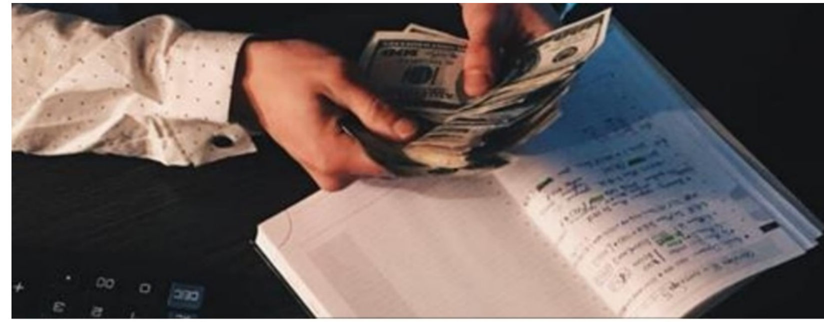
Day One ICO Trading Results

			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

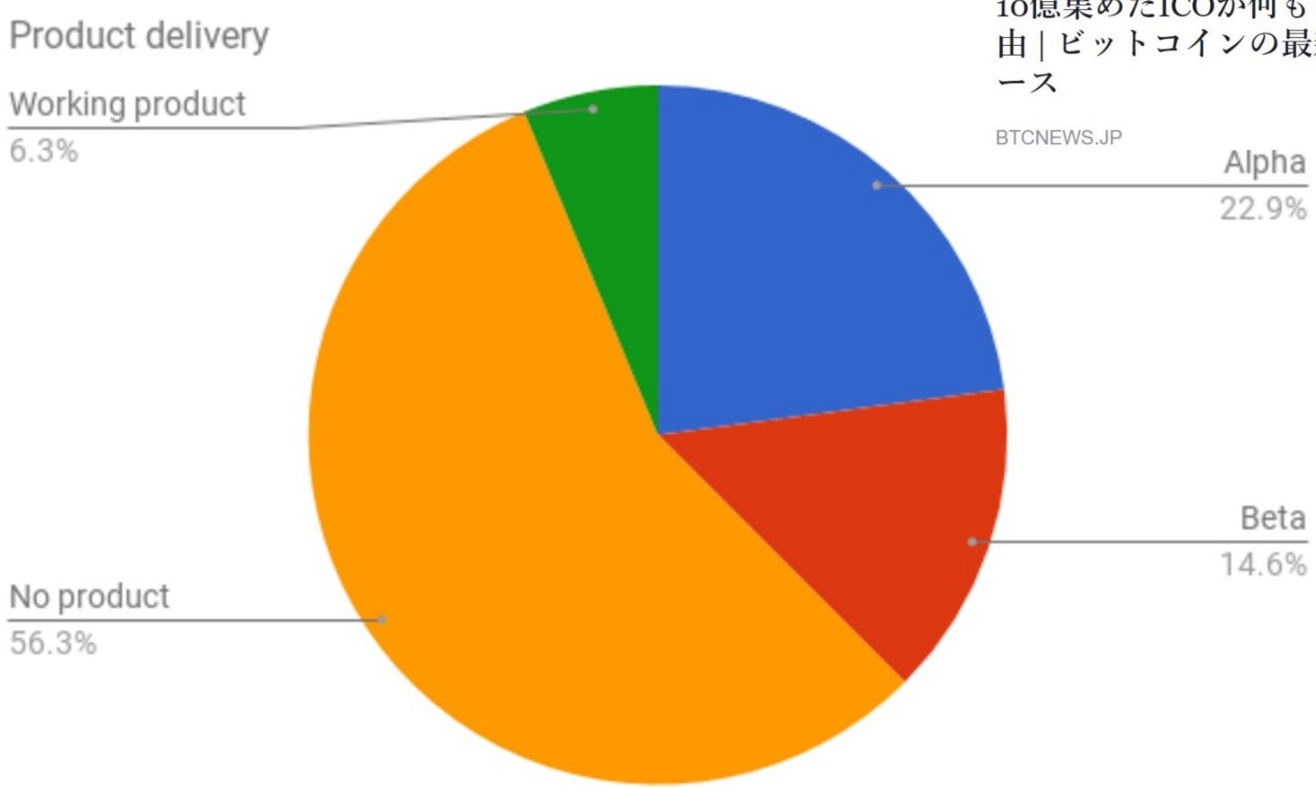
ICOの半数以上（56％）は まだ何かしらのプロダクトすら存在しない

- 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

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

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

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、多くの人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、多くの人が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

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。

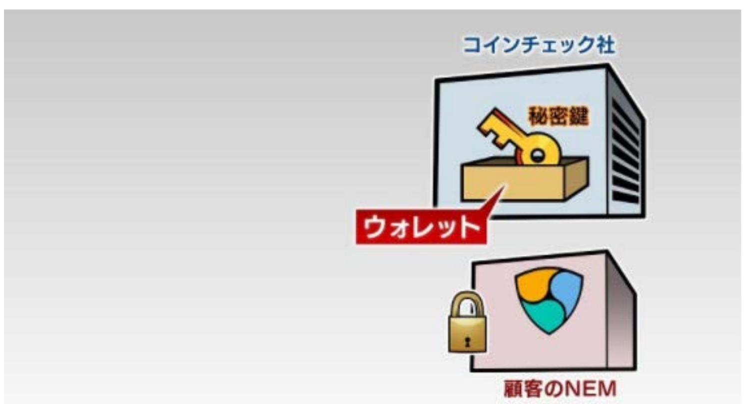
（注）ＩＣＯにより調達した資金の使い道（実施するプロジェクトの内容等）やトークンの販売方法などをまとめた文書をいいます。

○　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。

5. コインチェック事件と取引所セキュリティ

NHK 視点・論点「仮想通貨 不正流出事件の行方」

- 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	NA6JSWNE24Y
2018/1/26 3:28	100,000,000	NC4C6PSUW5	NDDZVE32WB
2018/1/26 3:18	100,000,000	NC4C6PSUW5	NB4QUCLTZW
2018/1/26 3:14	100,000,000	NC4C6PSUW5	NDZZJBH6JZP
2018/1/26 3:02	750,000	NC4C6PSUW5	NBKLOYXFIVF
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWFIZ
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

取引所セキュリティを考える視点

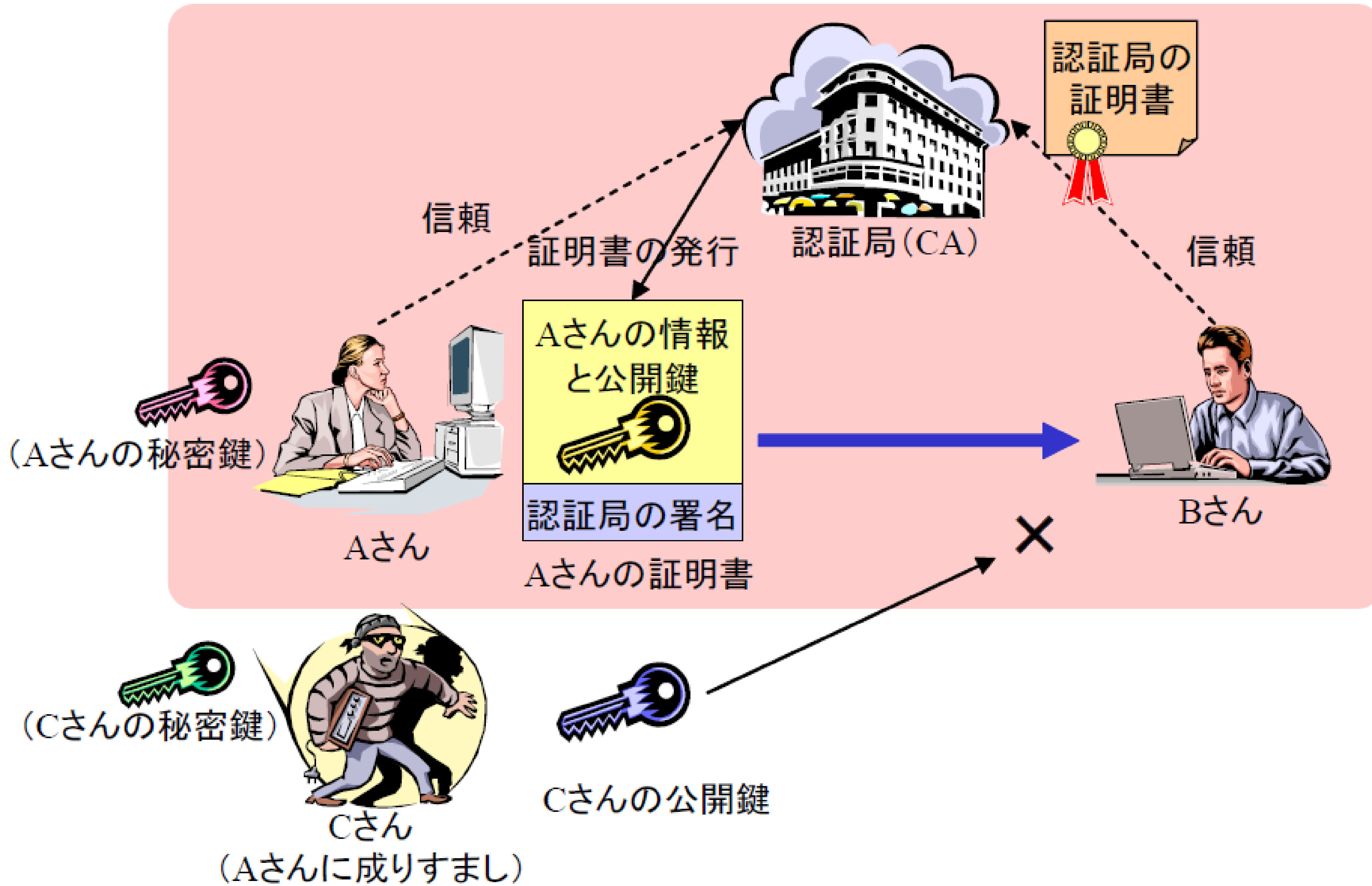
- 仮想通貨法は、取扱業者が多額の顧客資産を預かる存在であることを意識した、十分な利用者保護の仕組みを備えていない。
- 投資家・消費者保護の視点からの法規制の強化が必要か。
- 信託や保険の仕組みを活用した制度的な対策。
- 統一的なセキュリティ基準、経営体制やガバナンス、セキュリティ対策の充足状況に関する情報開示。
- オフチェーン取引による「トラストレスの中のトラスト」構造の問題。

「非中央集権」という設計思想

- ビットコインの持つ基本的な設計思想＝「非中央集権」
  - 信頼できる中央機関を決して置かないというポリシー。
  - 仮想通貨は、こうしたポリシーを持つからこそ、法律や政治体制の違いによる国境の壁をやすやすと越えて、国際的な利用が可能になった。
- 政府、中央銀行、裁判所といった信頼できる中央機関の存在を前提に構成された普通の世界から見ると、仮想通貨の世界は、きわめて特殊で危なっかしい。
- 今回流出したネムも、信頼できる中央機関を持たないというポリシーを持つ仕組みであるために、国家機関を含めて、何者も情報を恣意的に書き換えることはできない。
- こうした仮想通貨という異質な存在を、国家が適切に制御することが可能か。

６．トラストとトラストレスの狭間で

信頼できる第三者(CA)が存在する方式＝「トラスト」

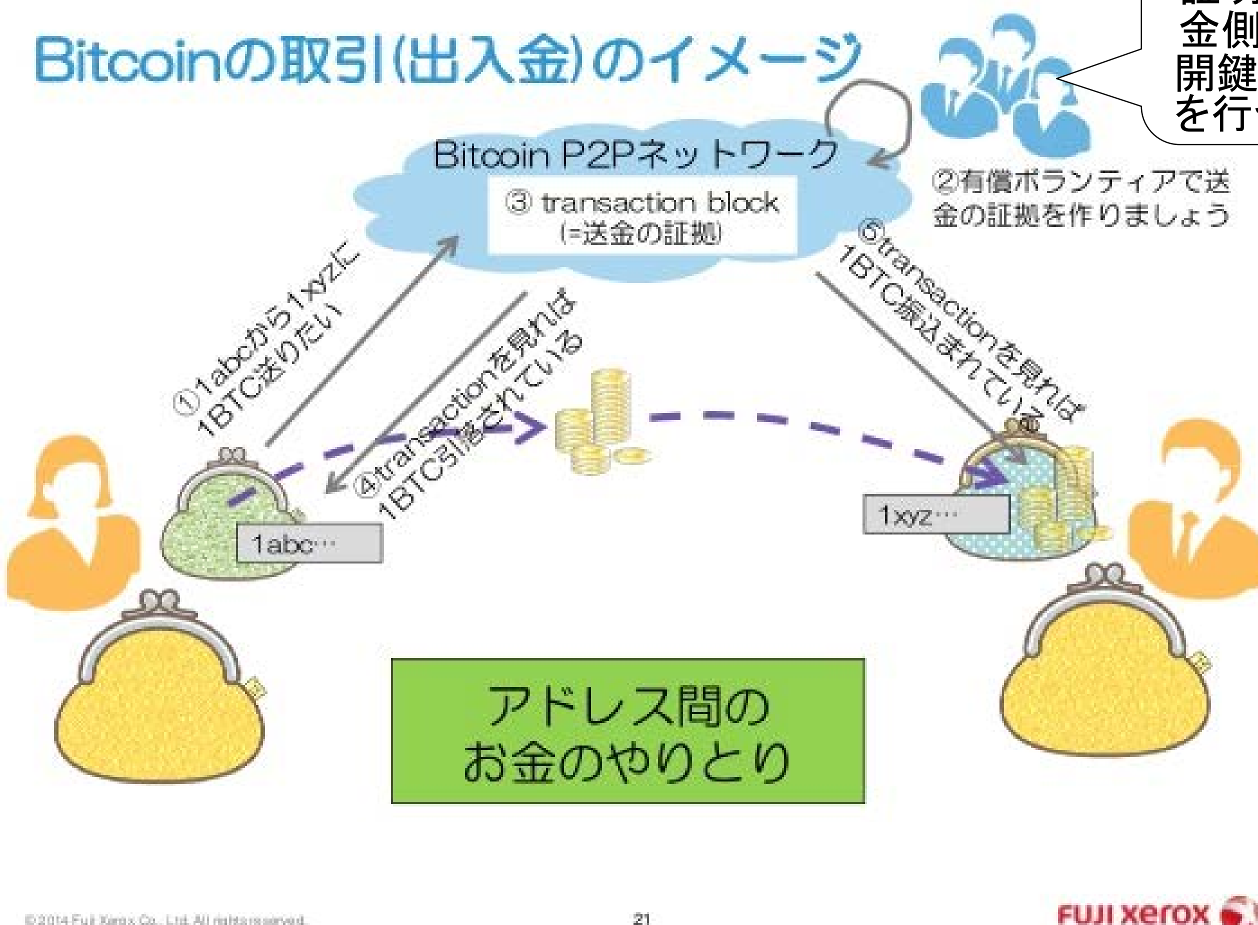


（出典） IPA、「PKI関連技術解説　v1.05」、2002.3.18

信頼できる第三者が存在しない方式＝「トラストレス」

ビットコインの取引においては、あえてPKIを使わず、公開鍵をそのままアドレスに使用することで、信頼できる第三者機関を置かない、センターを置かないというポリシーを貫いている。

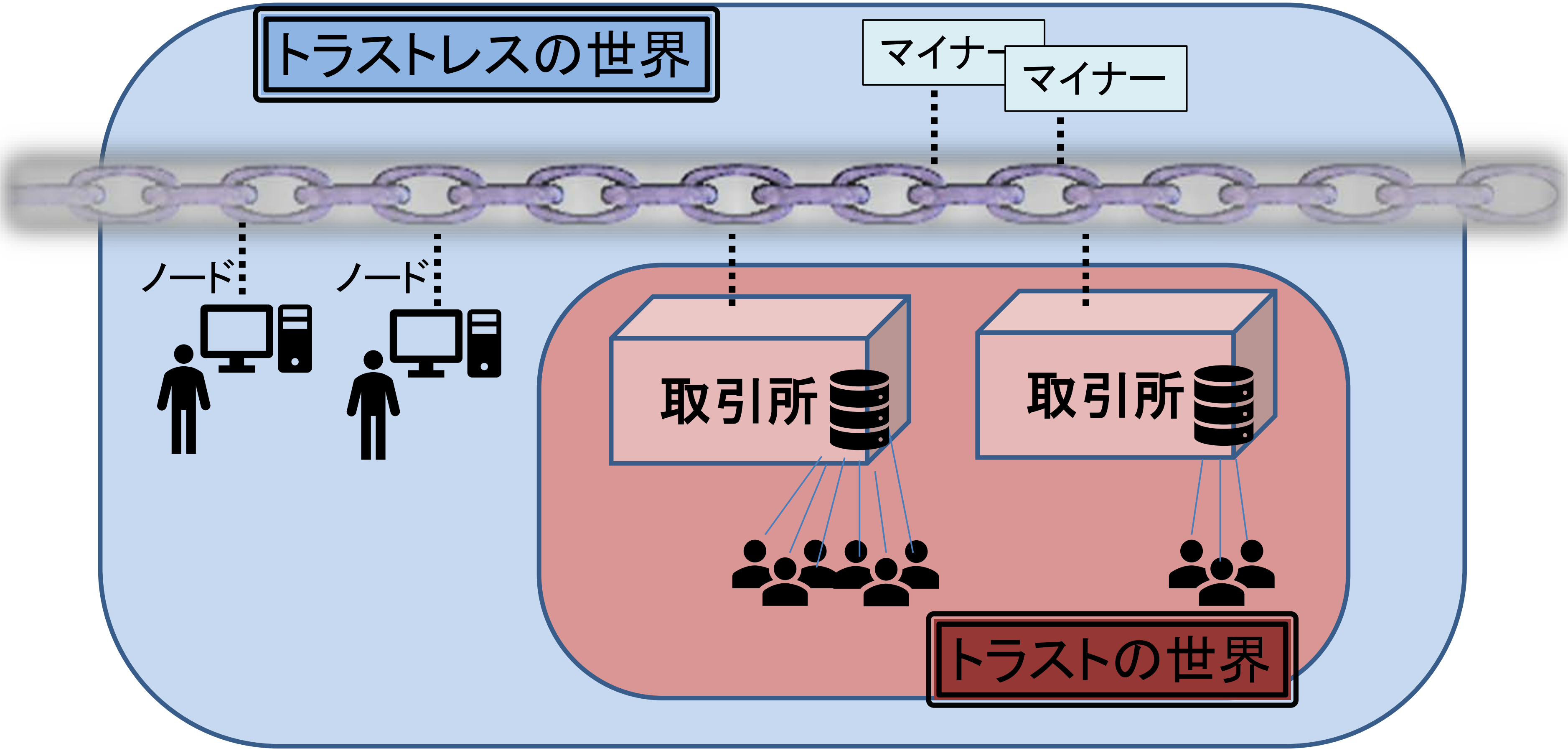
マイナーは、公開鍵証明書がなくても出金側のアドレスを公開鍵として署名検証を行うことができる。



（出典） 漆嶌賢二、「Bitcoinを技術的に理解する」、2014.6.2

でも、仮想通貨交換所は「信頼できる第三者」となっている

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。



「トラストレスの世界」の中に「トラストの世界」がある構造

サトシ・ナカモトの構築した世界

信頼できる第三者機関（センター）が邪魔だった。

- 運営コストが掛かる。
- SPOF（Single Point of Failure）となる。

センターを取り除くには、

→公開鍵をそのままアドレスに使用すればよい。

→その２つのメリット

- センターの運営費用が要らない。
- 匿名化（仮名化）できる。

⇒　これを「非中央集権」と呼んだことにより、政治的なメッセージ性を帯びることになる。

当初はそれでよかった

・利用者はギーク限定
・自分のマシンでマイニング
・鍵ペアも自分で生成
・秘密鍵も自分で管理

だから、「安価で安全なブロックチェーン」が作れた。

・利用者は自分で自分のシステムを守れる
・マイニングは多くの利用者のノードで分担
・秘密鍵の紛失や盗難は自己責任

⇒「トラストレス」の誕生

- すべてがオンチェーンの時代。
- 各利用者が秘密鍵さえ安全に管理していれば、信頼できる第三者は不要となった。

しかし、2013年頃から状況は変化する

- 利用者にビジネス関係者や個人投資家が混じるようになる。
- GPUやASICによるマイニング・ファームの誕生。
- 鍵ペアの生成も、秘密鍵管理も他人任せ

→守ってあげなければならない「弱い利用者」が生まれる。

取引所は「トラストレスの中のトラスト」

- 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。

取引所が一括して仮想通貨を混蔵保管する仕組みの発達

- オフチェーン取引が圧倒的多数になる。
- そうでなければ、百万人単位の利用者を管理できない。
- Bitfinex事件は、そうした限界から発生した。

⇒ それを守るためのコールドウォレット導入が進む。

トラストレスからトラストに逆戻り

BTC価格の上昇と共に、ブロックチェーンの運営コストも高価に
- 利用者側からセキュリティが破られる事例。
- マイニングパワーの偏り、51%攻撃、分裂騒動。
- 取引所自体がサイバー攻撃を受けるリスクの顕現化。

取引所が一括して利用者の仮想通貨を保護預かりするのであれば、取引所のセキュリティを銀行並みに高度化していかなければならない。

結局、トラストレスからトラストに逆戻り。

しかも、犯罪者側にはトラストレスのメリットが残る。
- NEMは結局取り戻せず、資金洗浄されてしまった。

再び、トラストレスの世界は来るか

それを可能にするためには、
・全ての利用者がギーク並みに精通する。
　→　無理。
・一般利用者でも簡単に管理できるコールドウォレットが普及。
　→　そのセキュリティは本当に守れるのか？
・秘密鍵管理が自分でできない利用者は離れていく。
　→　そういう判断ができる人ばかりではない。

いつの時代も消費者に受け入れられないものは廃れていく。
受け入れられるように進化したのが今の姿。
だとすれば、所詮は「非中央集権」は幻想ではないか。
元々はビットコインを構築するための技術的選択にすぎない。
「非中央集権」であることに価値がある訳ではない。

ブロックチェーンは魔法の杖ではない

仮想通貨については限界があるとして、それ以外の領域へのブロックチェーンの応用はどうなるのか？

コンソーシアム型ブロックチェーンでも、秘密鍵の管理は必要。しかし、ある程度の規模の企業であれば、セキュリティマネジメントはできるはず。そこに商機はありそう。

結局のところ、ブロックチェーンは、秘密鍵の管理を利用者に丸投げしただけであって、ブロックチェーンを使いさえすれば、セキュリティが守れる訳ではない。

ブロックチェーンは、秘密鍵の管理という責任に耐えられる利用者だけが使いこなすことができる技術と考えるべき。

⇒ ブロックチェーンは魔法の杖ではない。