国際政治経済懇談会

2020年10月20日

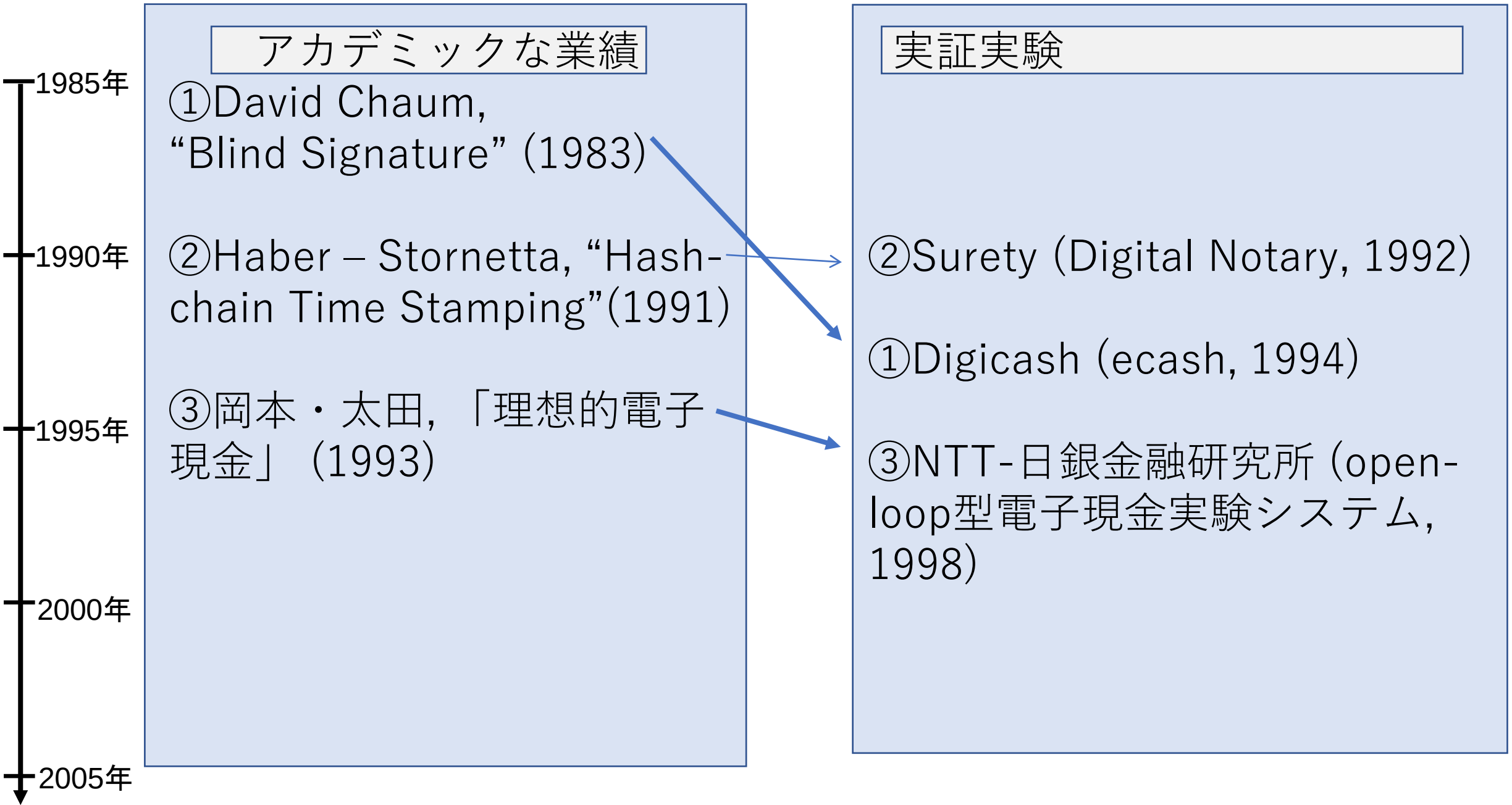
デジタル通貨を巡る論争を読み解く

京都大学 公共政策大学院

岩下 直行

Before the Bitcoin

Bitcoinに先立って開発されていた主な技術



David Chaum（1955 - ）

Digicash社のecash

ecashは、David Chaumが発明したblind signatureと呼ばれる暗号技術により、取引の匿名性を実現したclosed-loop型電子現金。

David Chaum
（1955 - ）

預金者

1.乱数xとrを生成
2.ハッシュ値$h(x)*r^e$を計算
3.$h(x)*r^e$を銀行に送信

7.$s[h(x)*r^e]*r^{-1} \bmod n$
$=[h(x)^d*r]*r^{-1} \bmod n$
$= h(x)^d \bmod n$
$=s[h(x)]$を計算
8.xとs[h(x)]を提示することで電子現金を支払えば、銀行の署名が検証できるが、xが銀行に還流しても匿名性を維持できる。

発行依頼

発行

支払い

銀　行

4.預金者の口座から引落
5.デジタル署名$s[h(x)*r^e]$
$=[h(x)*r^e]^d \bmod n$
$=h(x)^d*r \bmod n$を計算
6.$s[h(x)*r^e]$を預金者に送信

還流

加盟店

9.xとs[h(x)]を検証し受領
10.xとs[h(x)]を銀行に示し換金

注：　(e,n)及び(d,n)は、各々銀行のRSA暗号によるデジタル署名の公開鍵と秘密鍵。
r^{-1}は、$r \cdot r^{-1} \bmod n=1$となる正整数。

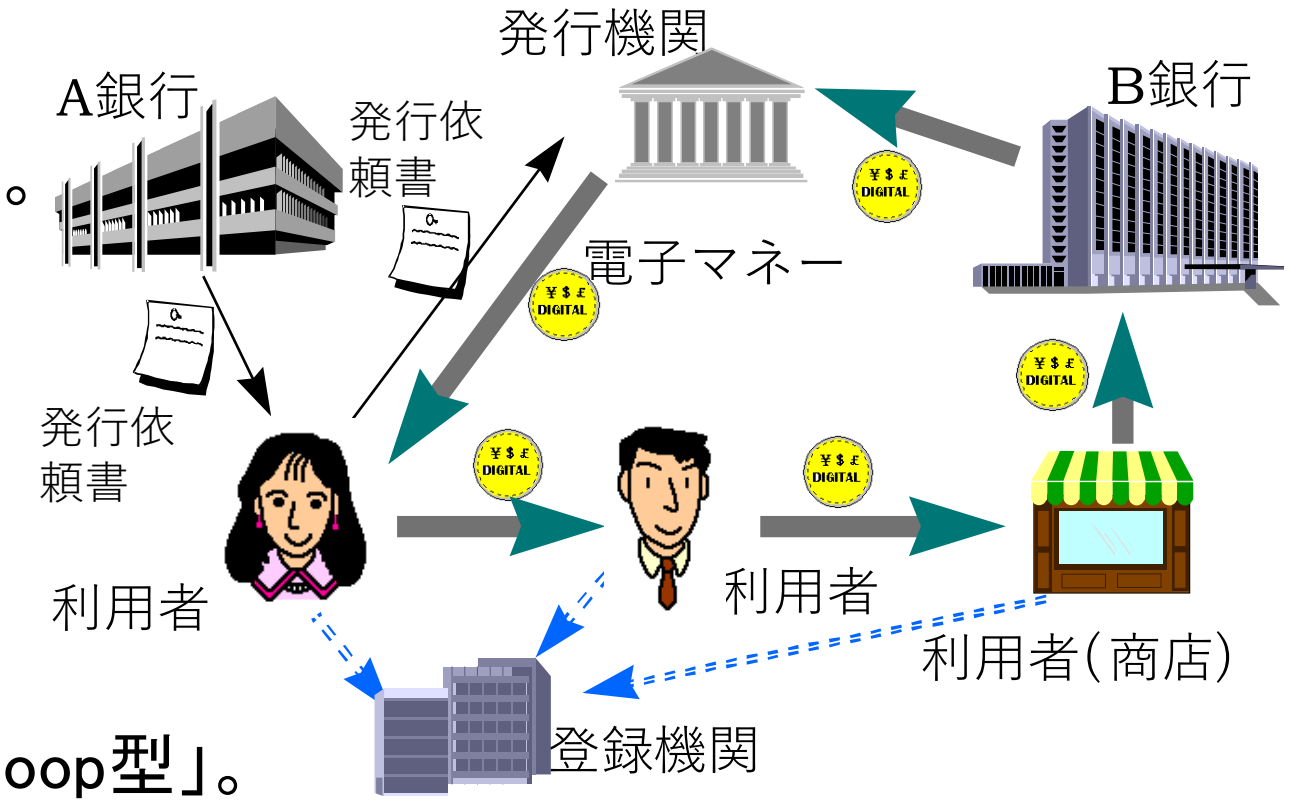
NTTと日銀金融研究所による電子現金実験システム（1998年）

（利用環境）

- コインを分割利用できる。
- ネットおよび商店店頭の双方で利用可能。

（セキュリティ対策の強化）

- ICカードの耐偽造性による事前対策と、電子マネーへの属性情報の埋め込みによる事後対策の二重の対策を組み込み。



（現金のメリットの継承）

- 利用者間での転々流通が可能な「open-loop型」。
- プライバシー保護の観点から、「取引の匿名性」を実現。

Bitcoin


$20.00 K
$15.00 K
$10.00 K
$5.00 K
$0
an '17
Jul '17
Jan '18
Jul '18
Jan '19
Jul '19
Jan '20
Jul '20

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

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstr
payme
financ
benefi
We pr
The n
hash-b
the pr
events
long a
attack
netwo
basis,
proof-

1. Introd

Commerce on t
trusted third pa

Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin v0.1 released

Satoshi Nakamoto

Announcing th
system that u
It's complete

See bitcoin.c

Download link
http://downlo

Windows only

- Unpack the
- Run BITCOIN
- It automati

If you can ke
you'll really

Abstr
payme
financ
benefi
We pr
The n
hash-b
the pr
events
long a
attack
netwo
basis,
proof-

1. Introd

Commerce on t
trusted third pa

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

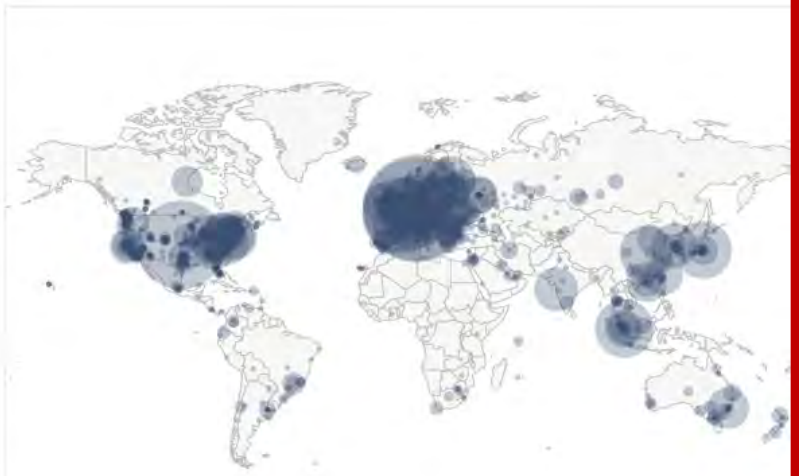
GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Oct 12 2020 03:19:06 GMT+0900 (日本標準時).

10744 NODES

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

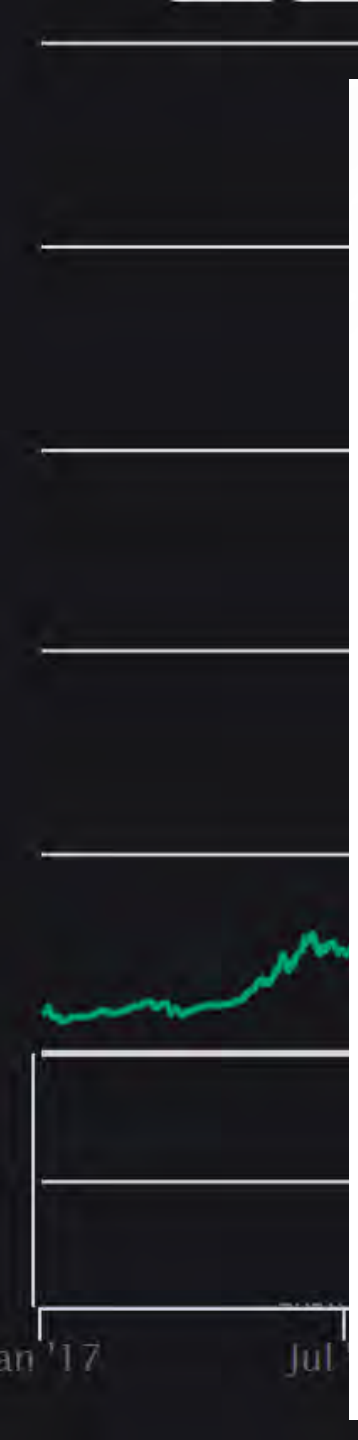
RANK	COUNTRY	NODES
1	n/a	2575 (23.97%)
2	Germany	1861 (17.32%)
3	United States	1839 (17.12%)
4	France	564 (5.25%)
5	Netherlands	419 (3.90%)
6	Canada	310 (2.89%)
7	United Kingdom	288 (2.68%)
8	Singapore	265 (2.47%)
9	Japan	224 (2.08%)
10	Russian Federation	222 (2.07%)



(source)bitnodes.earn.com/

$20.00 K
00 K
00 K
00 K
an '17

Stable Coins



#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$11,404.68	0.7%	0.55%	$211,220,873,033	$19,766,599,530 1,733,201 BTC	18,520,550 BTC	
2	Ethereum ETH	$372.21	1.38%	0.05%	$42,079,627,349	$11,124,319,880 29,887,377 ETH	113,054,076 ETH	
3	Tether USDT	$1.00	0%	0.03%	$15,831,452,927	$31,183,951,372 31,155,410,486 USDT	15,816,963,304 USDT	
4	XRP XRP	$0.242000	0.3%	5.38%	$10,950,010,666	$1,087,492,293 4,493,778,092 XRP	45,248,061,374 XRP	
5	Bitcoin Cash BCH	$247.49	0.8%	3.97%	$4,590,506,307	$2,121,661,982 8,572,614 BCH	18,548,025 BCH	
6	Binance Coin BNB	$30.76	1.83%	9.12%	$4,441,494,468	$417,171,355 13,563,516 BNB	144,406,561 BNB	
7	Chainlink LINK	$10.77	1.92%	2.72%	$4,186,161,784	$786,026,368 72,949,583 LINK	388,509,556 LINK	
8	Polkadot DOT	$4.06	3.25%	4.18%	$3,461,667,723	$201,807,055 49,707,348 DOT	852,647,705 DOT	
9	Cardano ADA	$0.105881	0.21%	0.15%	$3,294,218,903	$425,491,945 4,018,588,928 ADA	31,112,484,646 ADA	

Stablecoins

#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$11,404.68	▲ 0.7%	▲ 0.55%	$211,220,873,033	$19,766,599,530 1,733,201 BTC	18,520,550 BTC	
2	Ethereum ETH	$372.21	▲ 1.38%	▼ 0.05%	$42,079,627,349	$11,124,319,880 29,887,377 ETH	113,054,076 ETH	
3	Tether USDT	$1.00	▼ 0%	▼ 0.03%	$15,831,452,927	$31,183,951,372 31,155,410,486 USDT	15,816,963,304 USDT	

#	Name	Price	Market Cap	Volume	Velocity	Circulating Supply
3	Tether	$1.0000	$15,831,452,927	$31,183,951,372	1.97	15,816,963,304 USDT
12	USD Coin	$1.0000	$2,706,490,971	$319,457,137	0.12	2,705,255,498 USDC
26	Binance USD	$1.0000	$809,829,491	$214,296,483	0.26	809,505,689 BUSD
43	TrueUSD	$1.0000	$353,591,437	$53,862,864	0.15	353,345,284 TUSD
71	HUSD	$1.0000	$142,312,563	$21,237,600	0.15	142,243,692 HUSD
24	Dai	$1.0100	$912,368,853	$62,428,111	0.07	902,549,880 DAI
59	Paxos Standard	$1.0100	$246,205,072	$304,627,743	1.24	244,951,954 PAX
	Total		$21,002,251,314	$32,159,861,310	1.53	

Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
						18,520,550 BTC	
						113,054,076 ETH	
						15,816,963,304 USDT	

...city	Circulating Supply
...97	15,816,963,304 USDT
...12	2,705,255,498 USDC
...26	809,505,689 BUSD
...15	353,345,284 TUSD
...15	142,243,692 HUSD
...07	902,549,880 DAI
...24	244,951,954 PAX
...53	

Libra


$20.00 K
$15.00 K
$10.00 K
$5.00 K
$0
an '17
Jul '17
Jan '18
Jul '18
Jan '19
Jul '19
Jan '20
Jul '20

Libra

libra

An Introduction to Libra

White Paper • From the Libra Association Members

Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people.

This document outlines our plans for a new decentralized blockchain, a low-volatility cryptocurrency, and a smart contract platform that together aim to create a new opportunity for responsible financial services innovation.

Problem Statement

The advent of the internet and mobile broadband has empowered billions of people globally to have access to the world's knowledge and information, high-fidelity communications, and a wide range of lower-cost,

libra

An In

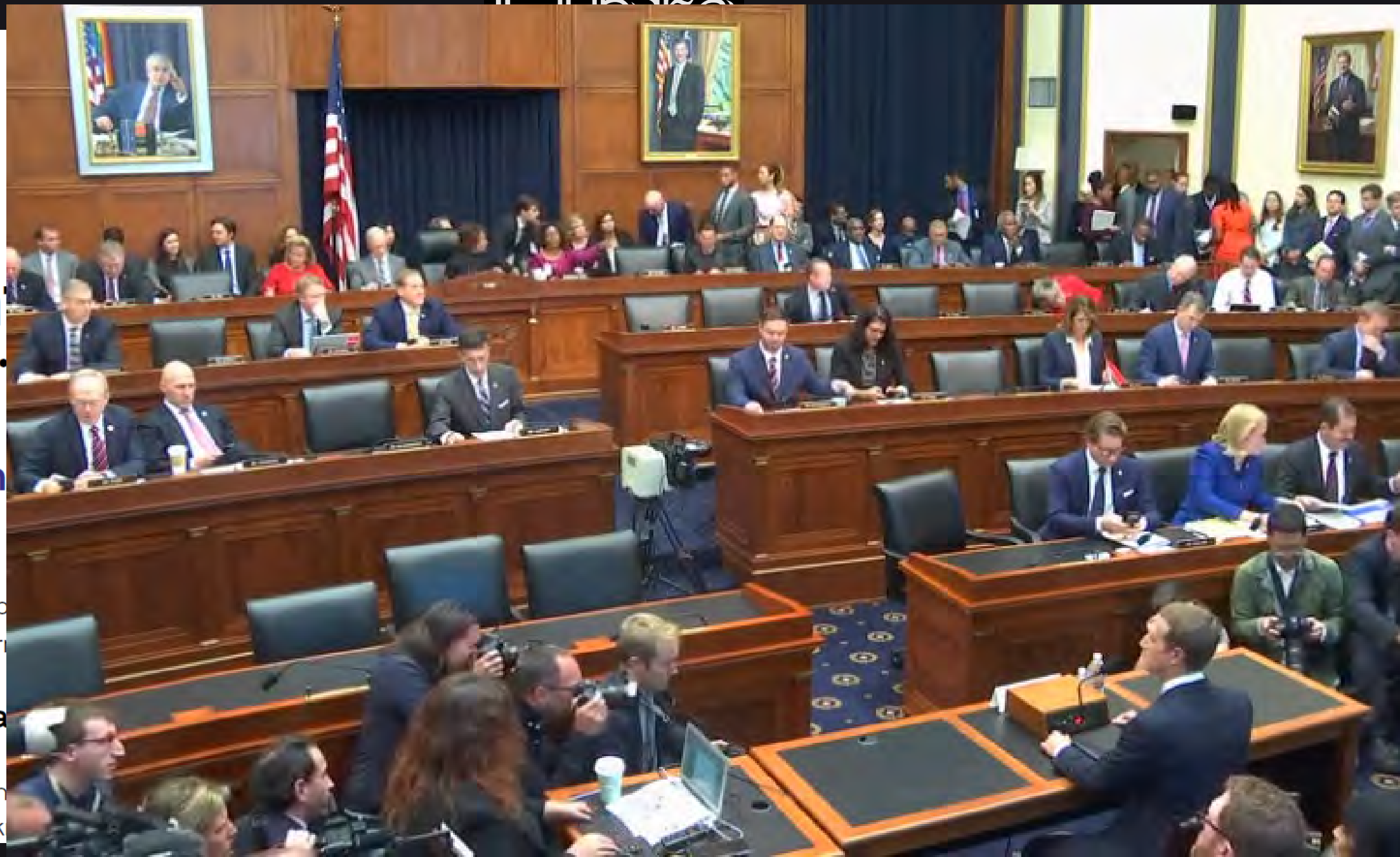
White Paper •

Libra's m
financial

This document c
contract platfor

Problem Sta

The advent of th
to the world's k



libra

An In

White Paper •

Libra's m
financial

This document c
contract platfor

Problem Sta

The advent of th
to the world's k

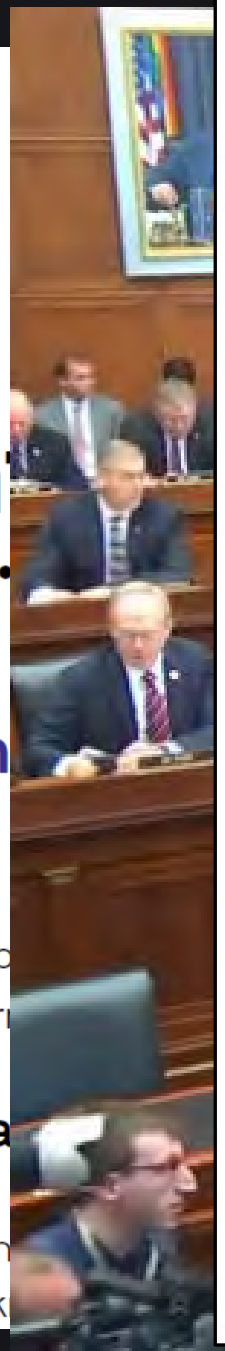
Libra
@Libra_

We have initiated the formal payment system licensing process with @FINMA_media and updated our white paper to reflect key design changes to the Libra payment system. bit.ly/2IVqWxg
#FinancialInclusion #TechforGood

ツイートを翻訳

午後11:00 · 2020年4月16日 · Sprout Social

390 リツイート　**783** いいねの数



Libra
@Libra_

2020年4月16日に公開された
新しいリブラ・ホワイトペーパーの
主な変更点は次の3点。

1.シングルカレンシー型ステーブルコインの追加
（事実上のドルペッグ）。

2.堅牢なコンプライアンスの構築（マネロン対策）。

3.将来的なパーミッションレス・ブロックチェーンへ
の移行を見送り。

CBDC


$20.00 K
$15.00 K
$10.00 K
$5.00 K
$0
an '17
Jul '17
Jan '18
Jul '18
Jan '19
Jul '19
Jan '20
Jul '20

CBDC

CCIEE Vice Chairman Says PBOC Will Be First to Roll Out Digital Currency

INDUSTRY David Lee October 28, 2019

$20.00 K
$15.00 K
$10.00 K
$5.00 K
$0

an '17
Jul '17

CBDC

Chairman Says PBOC Will Be First Digital Currency

October 28, 2019

$20.00 K
$15.00 K
$10.00 K
$5.00 K
$0

CBDC

菊谷ルイス　ブロックチェーン　2020/10/10 06:40

デジタル人民元の配布

中国の深セン市政府がデジタル人民元（DCEP）を試運転するために、合計1000万人民元（約1.5億円）に相当するDCEPを抽選の形で5万人に配布することがわかった。中国メディアSouth China Morning Postなどが報じた。

一人あたり200元（約3100円）の受け取り分となり、政府はこの配布プログラムを通してデジタル元を推進することを目的とする。

具体的に、政府が運営するブロックチェーンアプリ「iShenzhen」に登録した市民のみ抽選に参加することができる。今週の日曜日に当選者を発表する予定だ。当選者は「デジタル人民元アプリ」からe-ウォレットを開設し、受け取ることになるという。

02:19

Bank of England mulls digital currency as Chinese efforts surge

Shaurya Malwa · July 15, 2020 at 8:00 am UTC · 3 min read

有效管理定向资金

灵活管理您电子钱包

ックチェーン 2020/10/10 06:40

00万

抽選の形で5万人に配布すること

Morning Postなどが報じた。

取り分となり、政府はこの配布プロ

とを目的とする。

ーンアプリ「iShenzhen」に登録

る。今週の日曜日に当選者を発表

アプリ」からe-ウォレットを開設

し、受け取ることになるという。

02:19

Bank of England mulls digital currency as Chinese efforts

Shaurya Malwa · July 15, 2020 at 8:00 am UTC · 3 min re

有效管理定向资金

灵活管理您电

ックチェーン 2020/10/10 06:40

Search

Bloomberg

Cryptocurrencies

Brainard Says Fed Studying Potential for U.S. Digital Currency

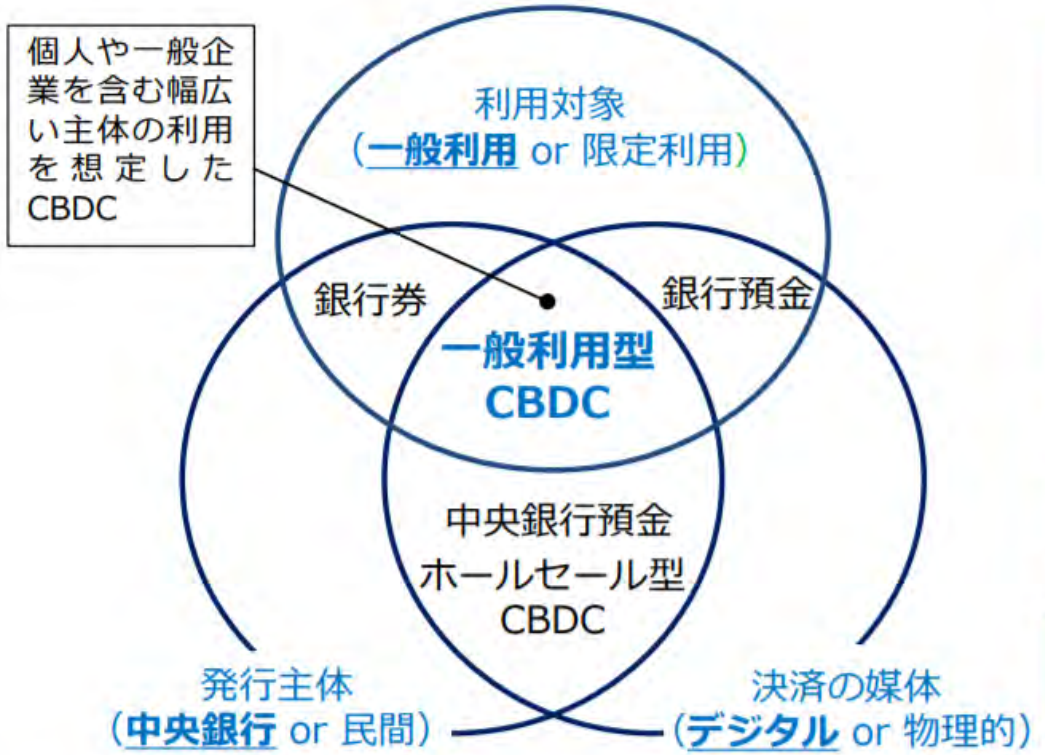
By Craig Torres and Vivien Lou Chen
2020年2月6日 6:10 JST

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

中央銀行デジタル通貨とは

- 「**中央銀行デジタル通貨**」（Central Bank Digital Currency：**CBDC**）とは、既存の中央銀行預金とは異なる、新たな形態の電子的な中央銀行マネー。
- **現時点でCBDCを発行する計画はない**が、**今後の様々な環境変化に的確に対応できるよう、しっかり準備しておく**ことが重要。

通貨の分類



一般利用型CBDCに期待される機能と役割

1．現金と並ぶ決済手段の導入

2．民間決済サービスのサポート

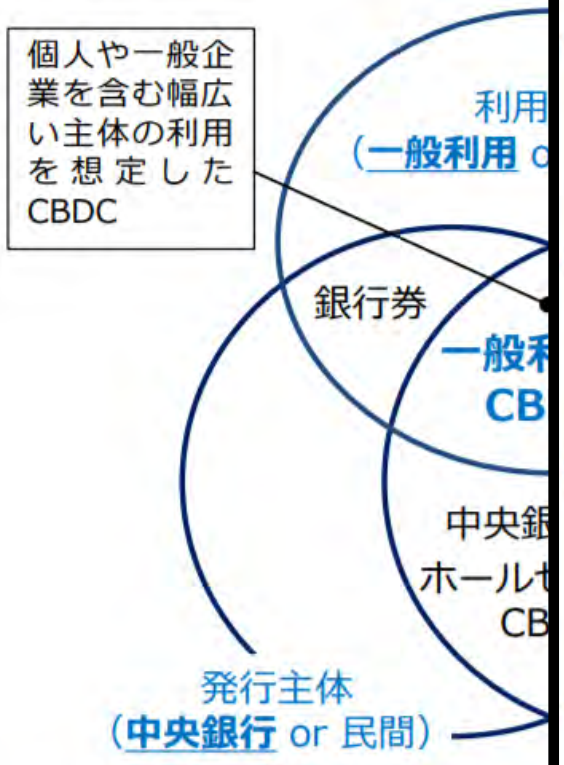
3．デジタル社会にふさわしい決済システムの構築

現金に対する需要がある限り、現金の供給についても責任をもって続けていく。

中央銀行デジタル通貨とは

- 「**中央銀行デジタル**
  既存の中央銀行預金
- **現時点でCBDCを発**
  できるよう、しっか

通貨の



今後の取り組み

- 今後は、これまでのようなリサーチ中心の検討にとどまらず、**実証実験**の実施を通じて、より具体的・実務的な検討を行っていく。
- 実証実験と並行して、CBDCの発行に関して考慮すべきポイントなどを踏まえ、**制度設計面の検討**を深めていく。内外関係者との連携も重要。

実証実験の流れ

概念実証フェーズ1
システム的な実験環境を構築し、CBDCの基本機能（発行、流通、還収）に関する検証を行う。
→2021年度の早い時期の開始を目指す。

概念実証フェーズ2
フェーズ1で構築した実験環境にCBDCの周辺機能を付加して、その実現可能性などを検証する。

パイロット実験
概念実証を経て、さらに必要と判断されれば、民間事業者や消費者が実地に参加する形でのパイロット実験を行うことも視野に入れて検討。

考慮すべきポイント

- **物価の安定や金融システムの安定との関係**
- **イノベーションの促進**
- **プライバシーの確保と利用者情報の取扱い**
- **クロスボーダー決済との関係**