中国人民银行
THE PEOPLE'S BANK OF CHINA

Technical Aspects of CBDC in a Two-Tiered System

YAO Qian

Institute of Digital Money,
People's Bank of China

CONTENTS

1、Central banks research on CBDC

中国人民银行
THE PEOPLE'S BANK OF CHINA

Similar to paper money	Different from paper money
Digital Base Money —claim on central bank	Digital Base Money—digitalized debts of central bank

Central banks of major economies devoted to research on digital currency

Bank of England

- Core studies in 2015. Focus on impact of CBDC on macro economy. Released The Macroeconomics of Central Bank Issued Digital Currencies in 2016.
- Research on DLT to support technical aspects of CBDC.

Bank of Canada

- Add CBDC to research agenda.
- Initiated Project Jasper in mid-2016.
- Experimented to apply DLT in high value payment system.

Riksbank

- Announced a two-year project in Nov 2016.
- Will decide on whether to issue CBDC by end-2018.
- Current studies on technical, policy and regulatory aspects.

ECB

- Studied on design and technical issues of CBDC since Jan 2017.
- Joint Project Stella with BOJ since Dec 2016 to test DLT application in financial infrastructure.

Bank of Japan

- Current research on CBDC stays at technical level. Vice Governor of BOJ said to learn more about new technologies including DLT in Nov 2016.
- Joint Project Stella with ECB since Dec 2016.

Monetary Authority of Singapore

- Joint Project Ubin with R3 since Nov 2016 to study on using CBDC in payment and settlement on a distributed ledger.
- In 2nd phase of Project Ubin, MAS cooperated with Accenture in 2017 to explore whether DLT can realize certain RTGS functionalities.

2. Objectives of CBDC

Fake

Coinage technology

Depre-ciation

Value support

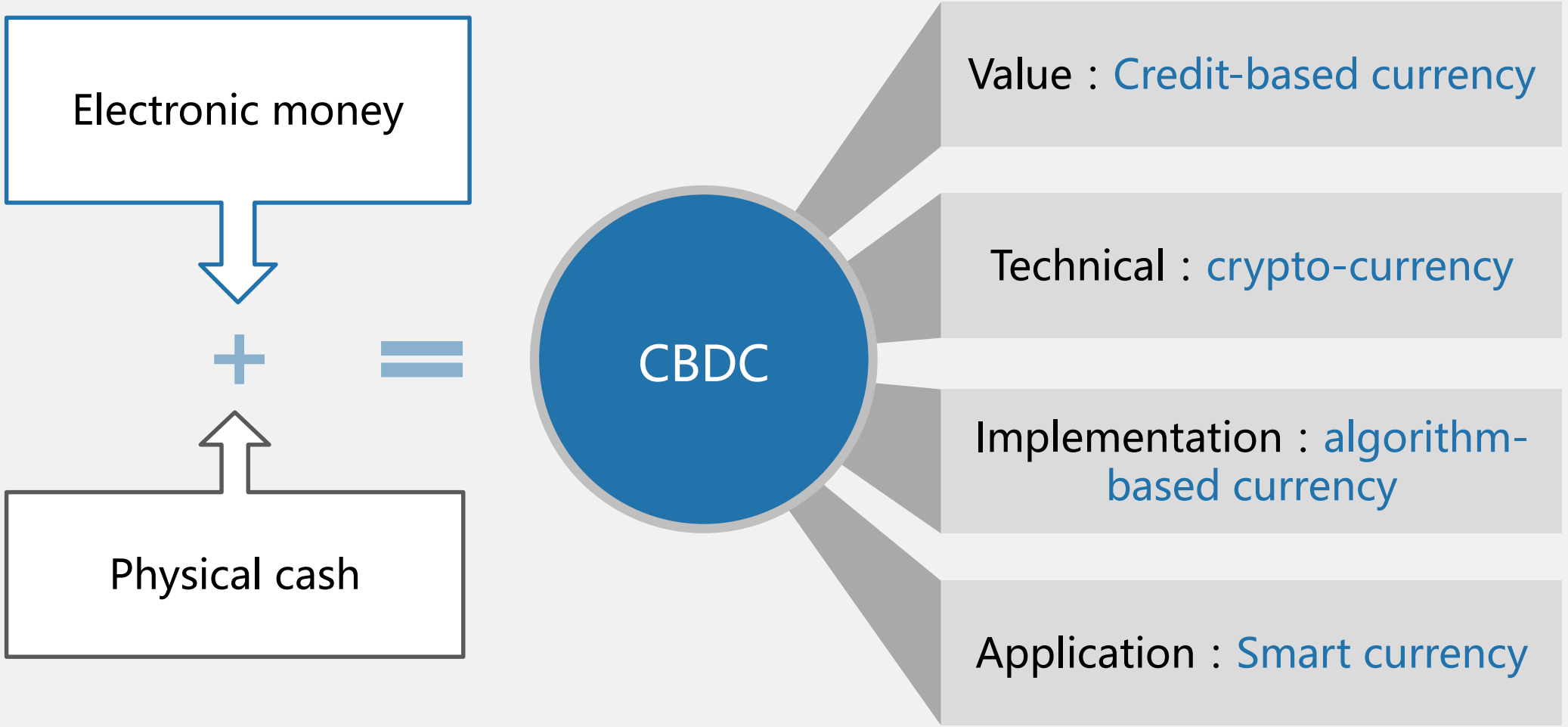
Objectives

- Higher value stability
- Higher data security
- Stronger regulation
- More flexible payment
- Smarter application

- Better service to the public
- More effective control measures
- Foundation of RegTech

姚前.理解央行数字货币：一个系统性框架[J].中国科学,2017,11.

3、Four dimensions of CBDC



4. Design principle of CBDC system

中国人民银行
THE PEOPLE'S BANK OF CHINA

Secure & Stable

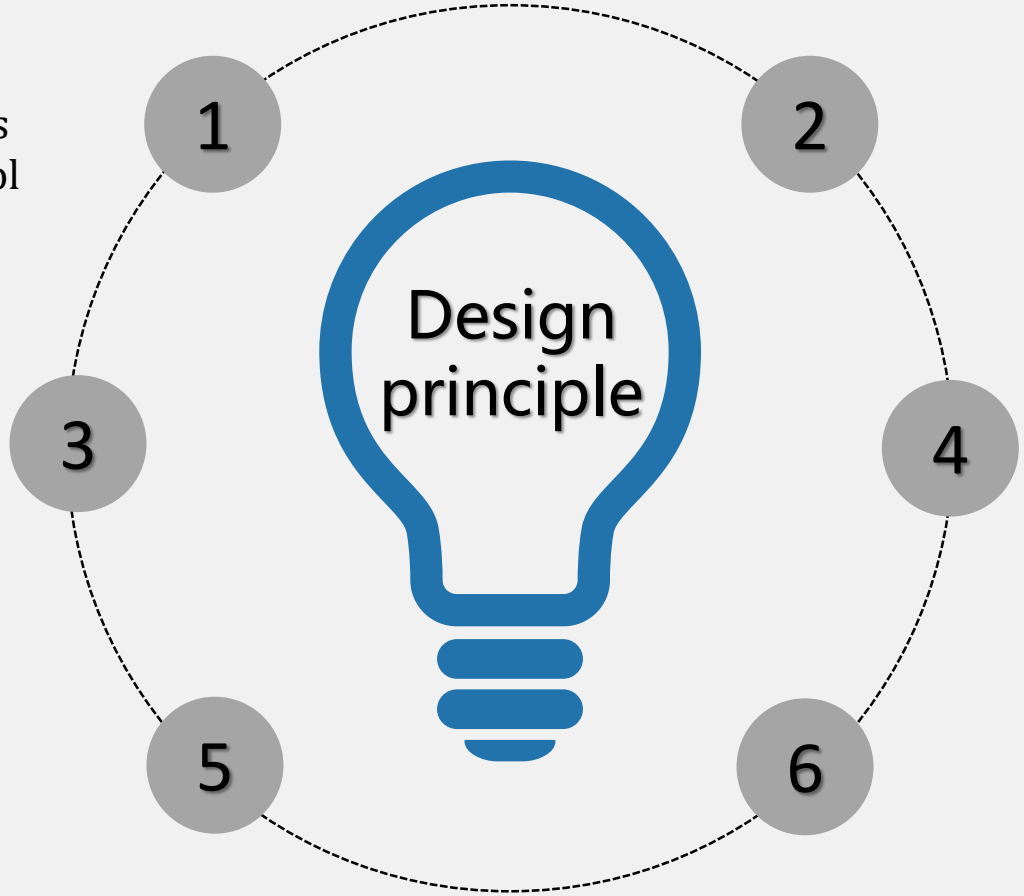
- Business objective analysis
- Security technology control
- Response measures

Proprietary & Controllable

- Proprietary design
- Proprietary development
- Proprietary integration

Neutral & Merit-based

- Technology neutral
- Competition and pick the best



Convenient & Efficient

- Process reinvention & optimization
- Support multiple scenarios

Tiered design

- Identify interests of all parties
- Loose coupled & tiered design
- Define interaction standards to enable regulated connection
- Centralized control & distributed architecture

Common development

- Integrity
- Closed loop
- Integrated development

CONTENTS

1.Evolution of traditional binary system

Chinese DFC: Theories and Architecture

中国金融 CHINA FINANCE 中国人民银行主管 半月刊

设为首页 | 加为收藏 | English

中国金融在线 在线报道中国金融

首 页 | 《中国金融》印刷版 | 关于我们 | 订 阅 | 投 稿 | 读者服务 | 中国金融文化研讨院

搜索 标题 金融危机 | 财经 | 房地产

- 要 闻
- 高端访谈
- 决策者说
- 观 点
- 热点专题
- 一线话题
- 视频/音频
- 金融市场
- 读 书
- 财经资料
- 职场人生
- 科技金融
- 银行业例行发布

扫一扫

在线浏览《中国金融》

首页 > 2016年第17期 > 专题：央行数字货币研究与探讨 > 正文

您好，欢迎来到《中国金融》，进入 [博客] [论坛]

中国法定数字货币的理论依据和架构选择

作者：范一飞

2016年09月01日 摘自：《中国金融》2016年第17期 共有0条评论

打印 Email 评论

近年来，数字货币热潮兴起，与之相关的一些底层技术，如区块链技术以及分布式记账方法，也显示出广阔应用前景。数字货币从理论走向现实，其必要性、可行性和安全性正在接受市场检验。以比特币为代表的某些类数字货币在私人部门率先得到应用。一些国家的中央银行也正在积极研究探索法定数字货币的制度设计和关键技术。作为中央银行，应基于维护金融体系稳定、促进金融创新、契合技术演进路径等因素综合考量，逐步实现法定数字货币的发行流通和对私人部门类数字货币的有效监管。

数字货币是历史发展的必然

货币演进中包含很多有趣现象。最初的以物易物是一种完全去中心化安排。但由于这种情形下的供需双重耦合很难，交易效率极低，极大地限制了贸易开展，也无法进行价值统一衡量。在"市场"推动下，货币媒介随之出现，并从开始的实物货币逐步过渡到贵金属货币，再到金银货币，货币形态和价值越来越趋于稳定，媒介范围也越来越广泛。实物货币、金银货币的发展经历了漫长历史，但因公信力问题，这类非中心化货币容易出现以假乱真、以次充好、缺斤少两现象。而随着国家法定货币的出现，人类才终于进入货币中心化时代。

纸币的出现是货币史上另一个巨大跨越。为解决金银货币存在的天然损耗、携带不便等问题，国家凭借公权力和公信力发行纸币替代实物货币。纸币一开始也锚定黄金或白银，以维持币值稳定和公众信心。后来人们发现纸币可以脱离金银而存在，于是纯信用货币出现，这是更为典型的中心化货币。纸币自身价值与票面价值相脱离，

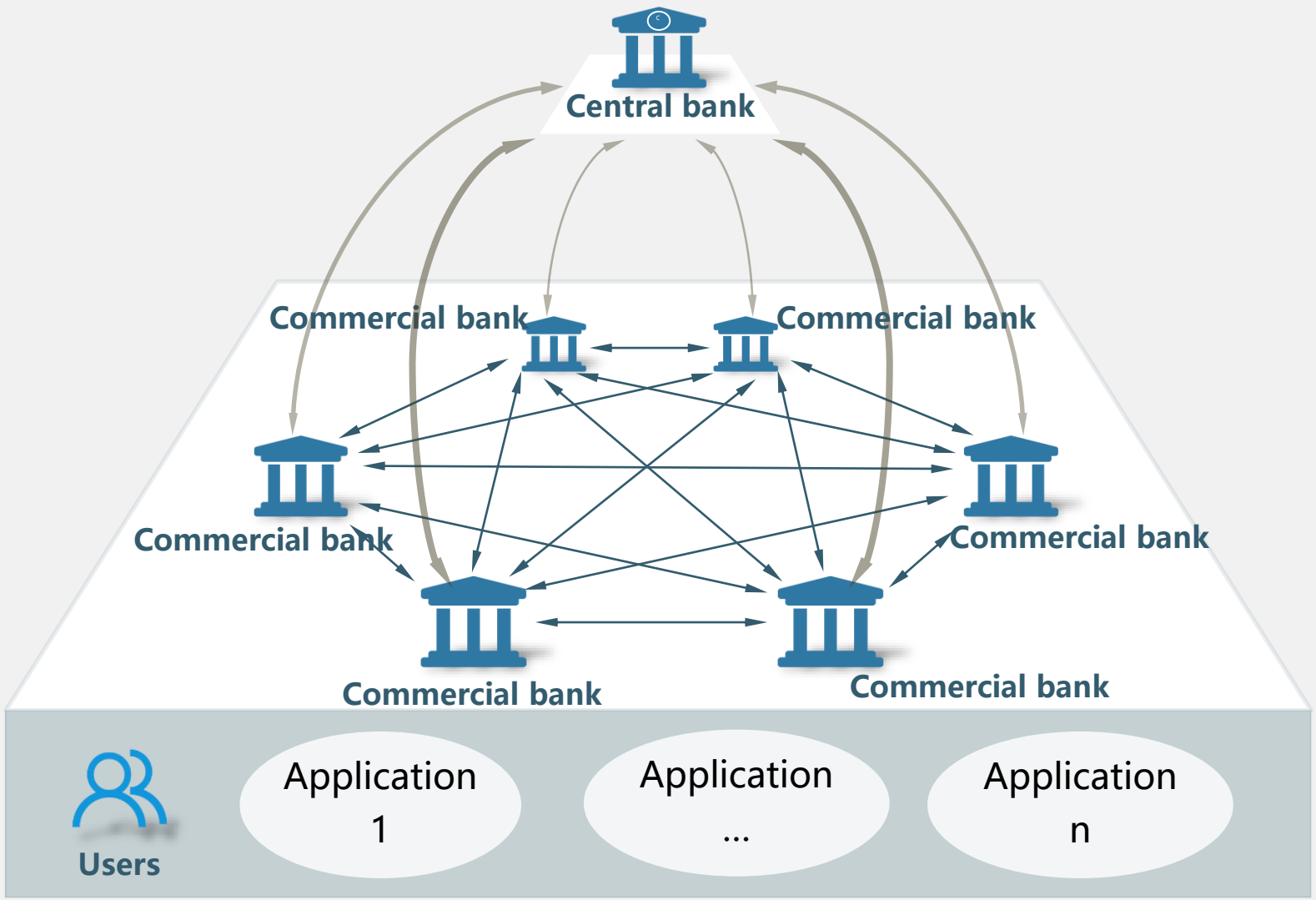
Two-tiered system

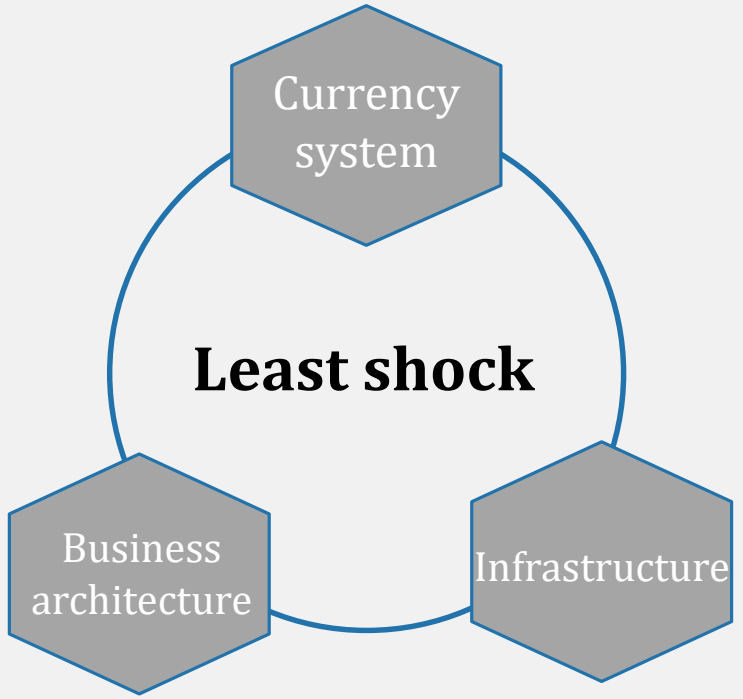
- Easy to replace physical cash
- Do not overturn existing system
- Incentives to banks
- Participation of banks
- Proper diversification of risks
- Accelerate service innovation

中国人民银行 THE PEOPLE'S BANK OF CHINA

Two-tiered system

Central bank – Commercial banks





Obtain / Recycle

Circulate

3. Business framework in a two-tiered system

中国人民银行
THE PEOPLE'S BANK OF CHINA

Business framework

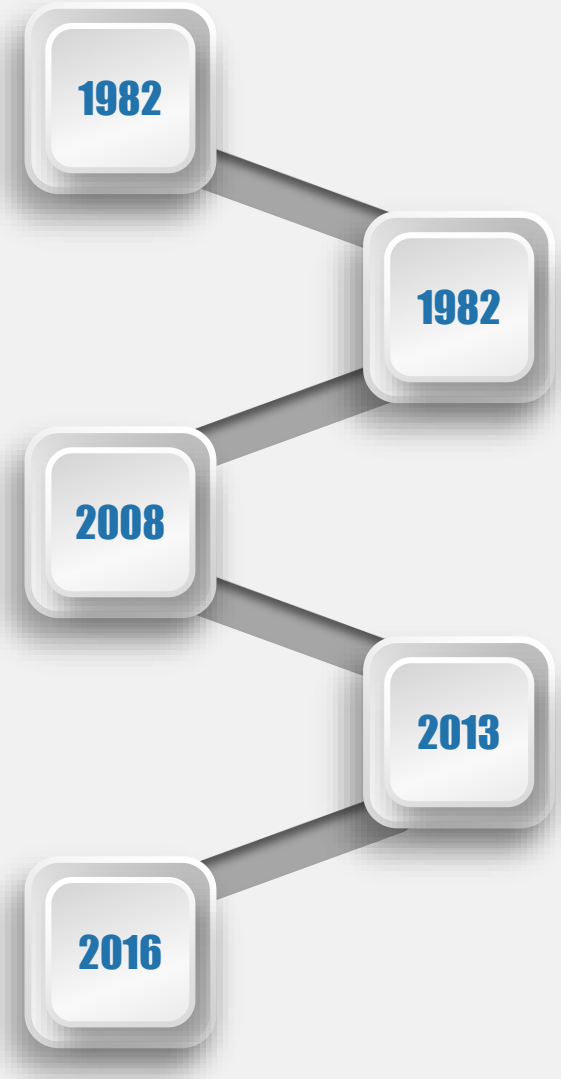
▼	Issue	Circulate	Retrieve	Manage & Control
Central bank	Issue Register	Ownership verification Liquidity mgt Transfer registration Error response Authorization mgt Emergency response	Retrieve	AML Risk mgt Audit Security Inter-connection Data analysis
Commercial bank	Obtain	Deposit & withdrawal Wallet Payment Operation User mgt Error response	Recycle	Risk mgt Data analysis Security KYC
End users		Deposit & withdraw Pay Log in Wallet		

CONTENTS

1. Form of presentation of CBDC

中国人民银行
THE PEOPLE'S BANK OF CHINA

‘Studies on encrypted digital currency began long time ago. Private quasi-digital currency emerged in recent years. Yet studies and application of encrypted DFC are scarce.’



David Chaum, the father of digital currency, was the first to propose an anonymous and untraceable electronic cash system.

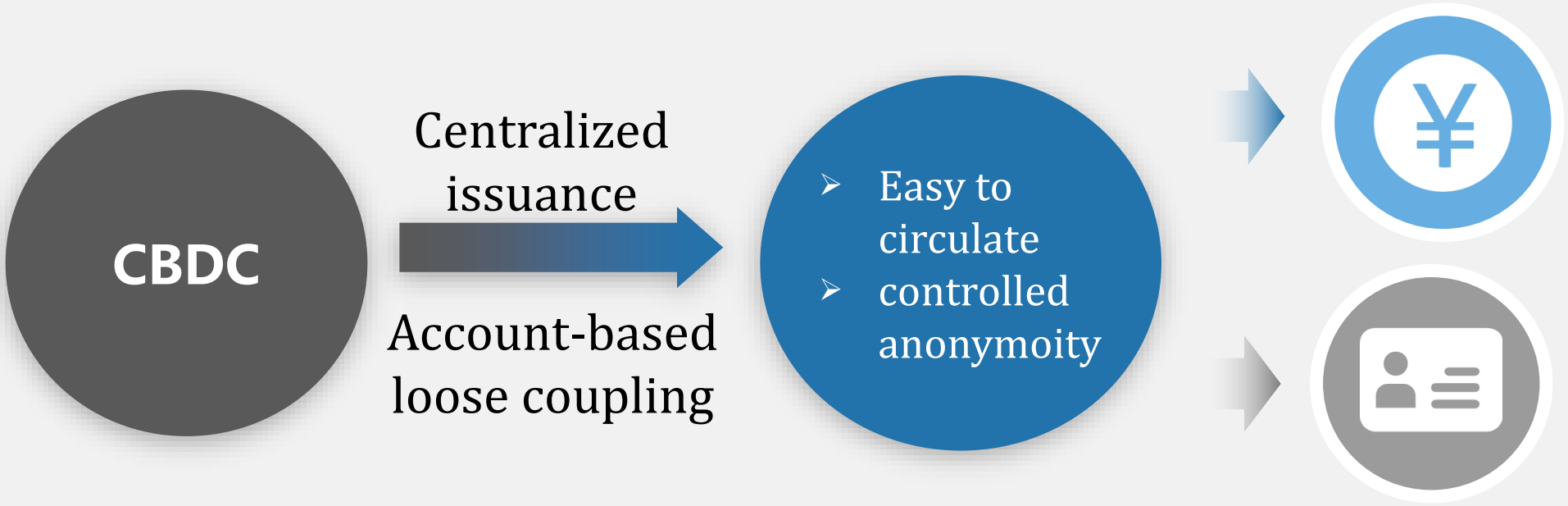
David Chaum founded the DigitCash and developed the E-Cash. He did research on certain features of digital currency and made important breakthroughs.

Satoshi Nakamoto published Bitcoin: A Peer-to-Peer Electronic Cash System where he proposed a decentralized solution for digital currency, the Bitcoin.

JP Koning proposed the FedCoin and provided solution for retail payment.

PBOC proposed an encrypted DFC solution.

2. Loose-coupling ①: Loosely coupled with bank accounts in terms of form



Number	+	Denomination	+	Application extension	Variable length	+	Programmable script	Variable length	+	owner	+	Issuer signature

Include basic features of fiat currency system (e.g. elements and rights) and extendibility.

Support structural horizontal layering and user-defined variable length with strong extendibility, able to meet various demands.

Support multiple DFC features such as one-time pad, programmability, unforgeability and tamper resistance.

3. Loose-coupling ②: Loosely coupled with bank account in terms of implementation

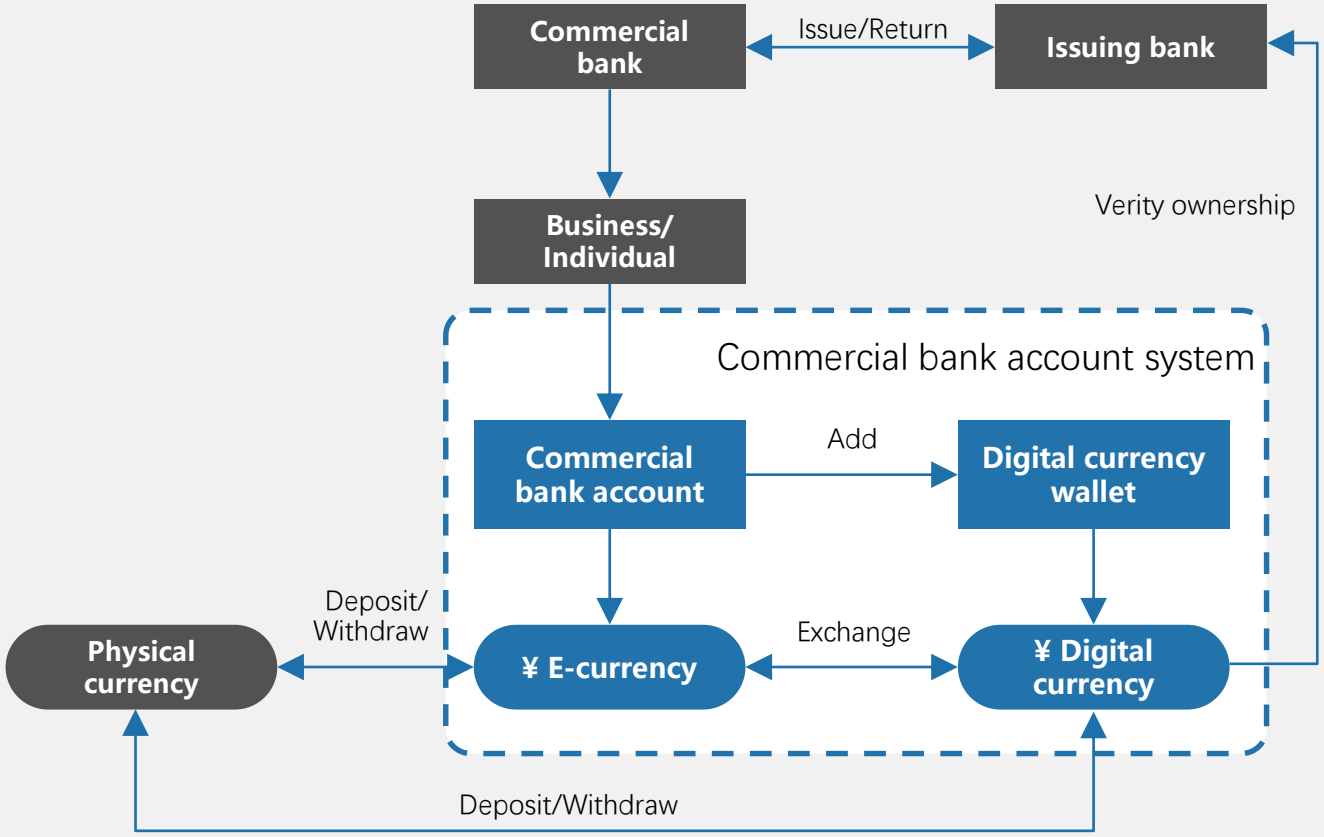
We understand bank account as an entire set of contracts that integrate all services provided by banks for customers.

- Multiple issuing agents with distinctive features
- Ownership or control of business logic
- Improve efficiency and provide dynamic service
- Not wasting existing IT resources

4.To realize loose-coupling with bank account: introducing digital currency wallet to bank account

中国人民银行
THE PEOPLE'S BANK OF CHINA

An implementation model: based on commercial bank account



Digital currency

Ownership of digital currency verified by agents

Greatly enhance KYC and AML capacity of banks

Traditional bank accounts

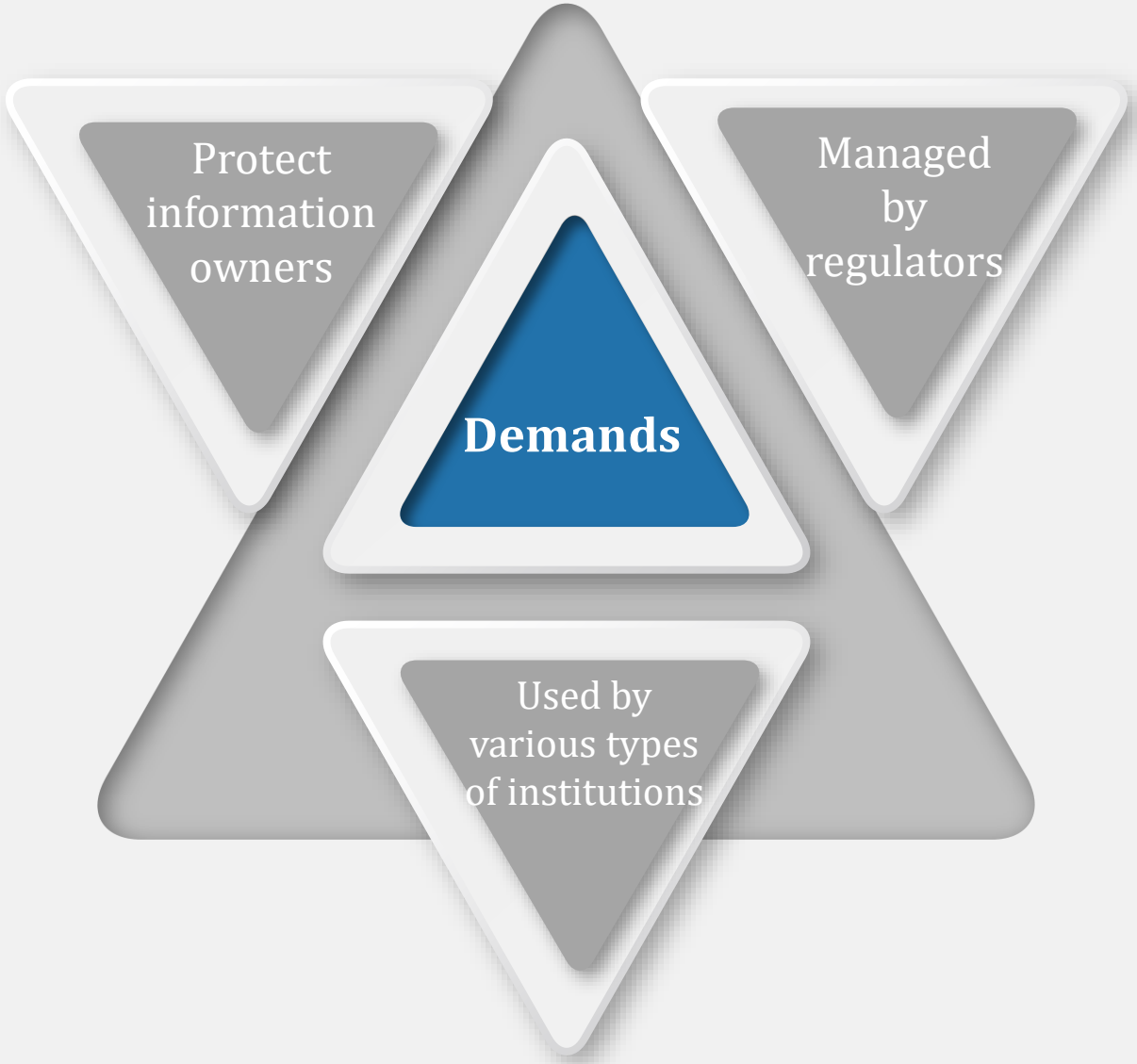
CONTENTS

1.Protect privacy of information owners via institutional arrangements

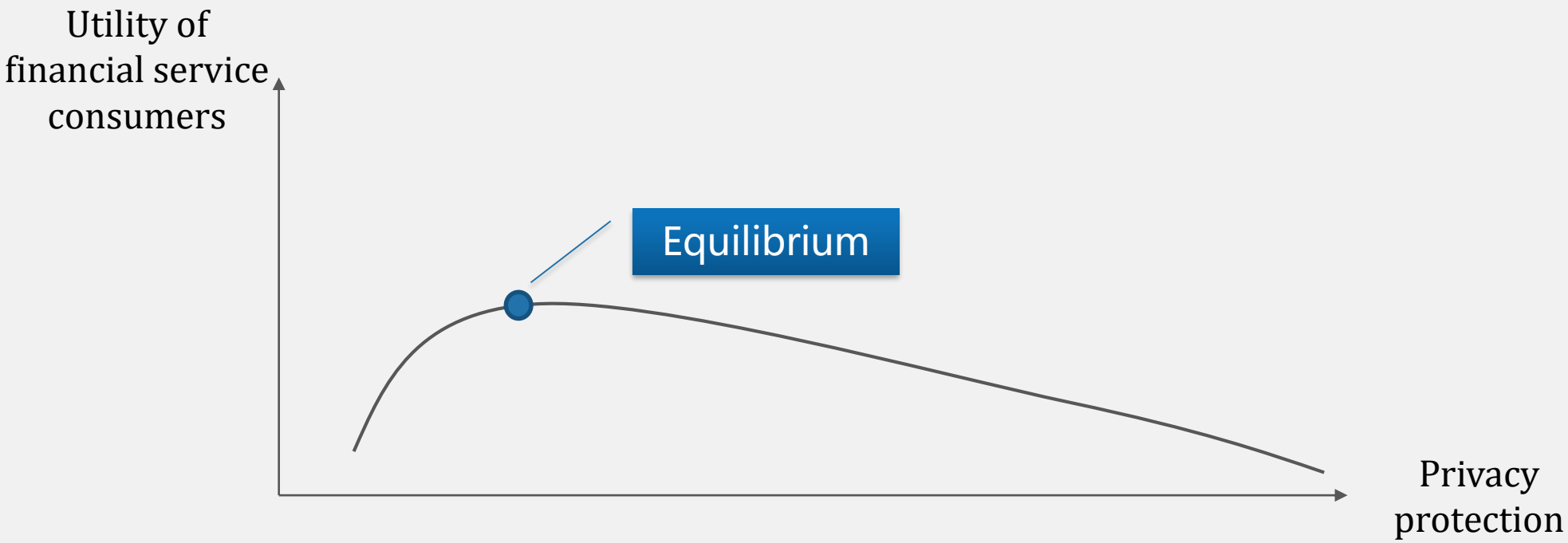
中国人民银行
THE PEOPLE'S BANK OF CHINA

Multiple players	• Clients • Financial institutions • Merchants • Payment service providers
Multiple procedures	• Collect • Use • Transmit • Destroy
Multiple means	• Clean • Integrate • Analyze • Mine

Privacy protection mechanism with controlled anonymity



2. Find optimal equilibrium for privacy protection



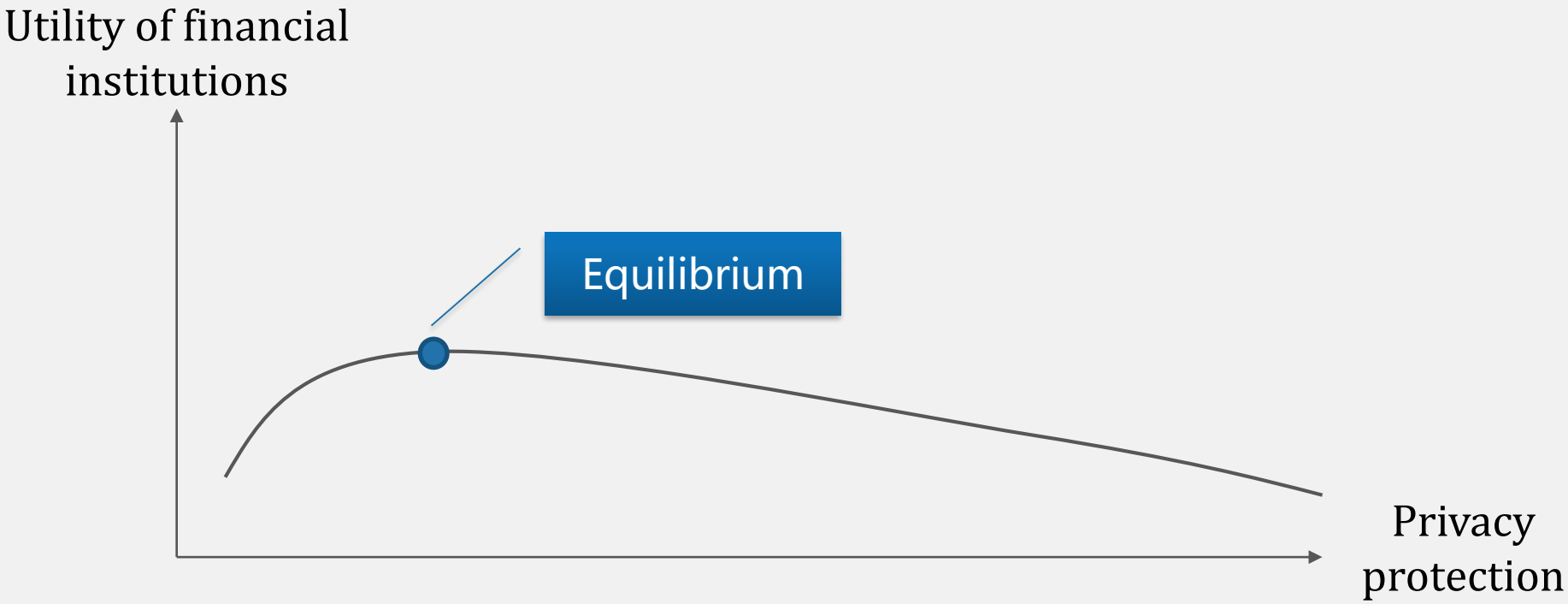
Consumer security not ensured
Unwilling to share or disclose information

Optimal equilibrium

Undermine financial activities
Weaker individual utility

Lowest **Highest**

2. Find optimal equilibrium for privacy protection



Consumer information stolen
Financial institutions' reputation impaired

Optimal equilibrium

Higher operation costs and application for financial institutions

Lowest **Highest**

3.Regulators manage information demands

Financial regulators as administrators of financial market order should ensure security of information of **financial consumers** and supervise **financial institutions** to use financial information effectively.

Not anonymous to anyone

↓

Personal info leakage

Allow complete anonymity to parties other than the trading parties

↓

Encourage tax evasion, money laundering

Legal protection

Protecting privacy of personal information with sound legal system is the prerequisite for CBDC to be accepted by the public.

Information identification

Tracking crime-related financial information may help to crack down on crimes and protect human rights and facilitate prevention and investigation of terrorist activities.

4.Controllable anonymity mechanism: definitions

Controllable

Identify real identities of trading parties and trading elements by collecting client information, verifying digital currency ownership and recording trading process, so as to realize traceability in certain situation and ensure that central bank gets the full information of digital currency.

Anonymous

Based on loosely-coupled accounts, privacy protection technologies are used to manage data access, so as to ensure anonymity of cash, meet demand of the public for anonymous payment service and ensure that parties in the circulation process can only access information related to themselves or meaningless data.

5.Controllable anonymity: Design principle & implementing technologies

Voluntary anonymity at front-end & Real-name at back-end

Technical measures are adopted to ensure that trading parties can only see the information voluntarily disclosed by the other party. Non-public information is protected and appears to be inaccessible.

Not individual-related info

Make financial information less identifiable. Cut off the connection between financial information and particular individuals, to make information "not-individual-related".

Proper disclosure of financial information

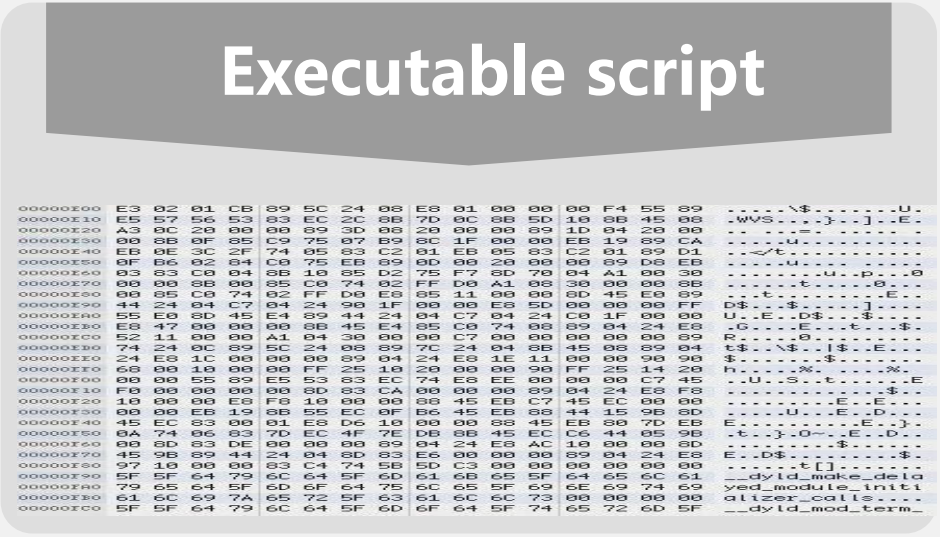
	Identity info	Financial trading info		Derivative info	Info access
		Trading elements	Trading scenarios		
Central bank	●	●	●	●	All clients
Counterparty	○	●	●	○	Counterparty
Agents	○	●	○	◎	Own clients
Commercial bank	●	○	○	◎	Own clients

●Accessible info
○ Inaccessible info
◎ Partially accessible info

CONTENTS

1.Two types of smart contract

Executable script embedded in digital currency



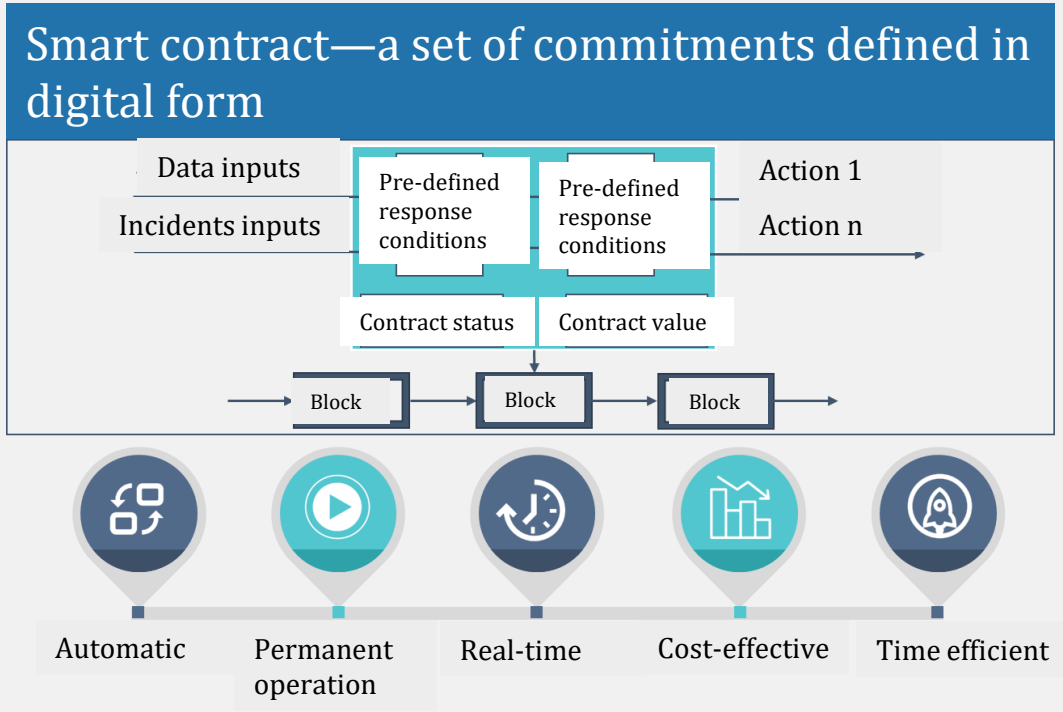
1 Extension of batch file

2 Programs saved as plain text

3 Similar to natural language

4 Facilitate rapid development & control

System-dependent smart contract



2.Be prudent about executable script and smart contract

Executable script

- Loose coupling
- Add fields of executable script
- Change form of presentation
- Prudence is required

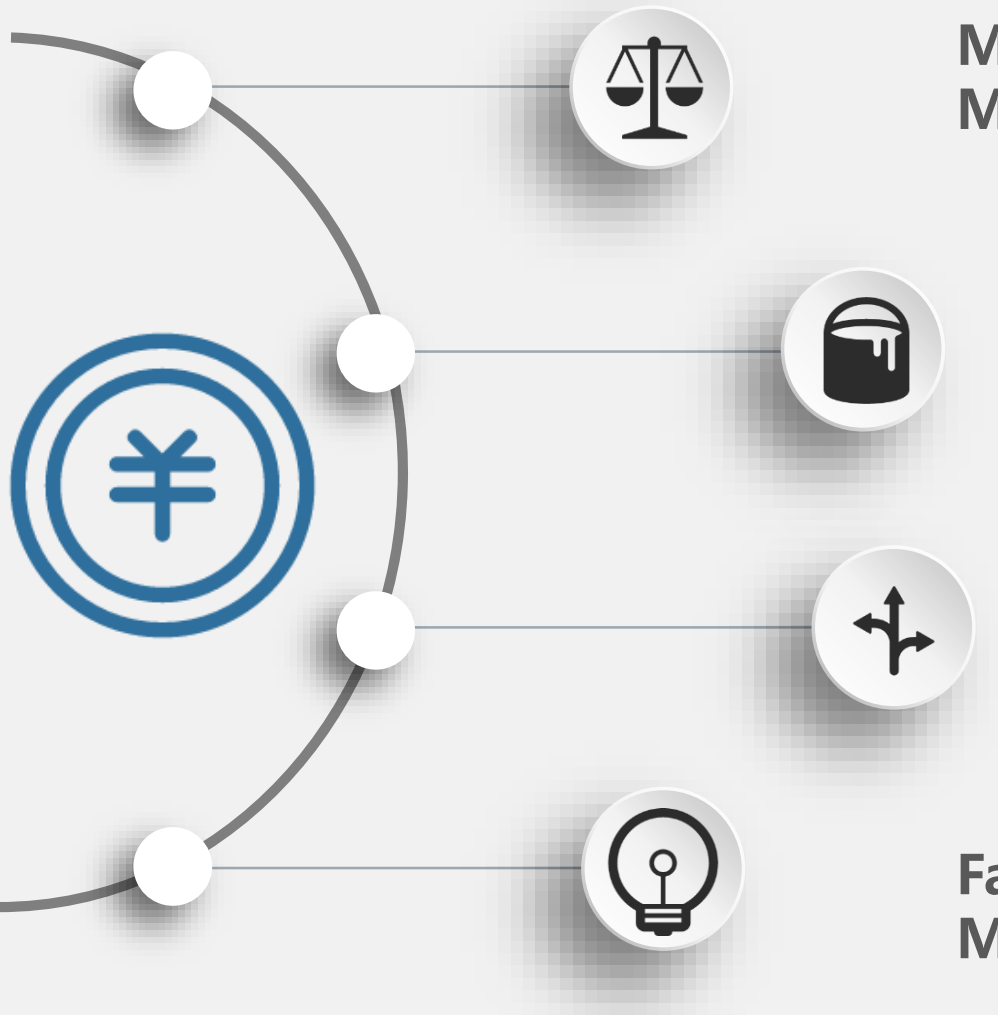
- Not change CBDC format
- Technology at early stage
- Immature implementation technologies
- Challenges in recovery and control
- Prudence is required

Smart contract

CONTENTS

VI 1.Market-driven competition & pick the best

中国人民银行
THE PEOPLE'S BANK OF CHINA



Market-driven competition & pick the best
Mobilize resources of commercial institutions

Synergy of resource integration
Avoid the Cannikin Law

De-centralized issuance model unlike that of any other tokens
No pre-determined technical routes; mobilize various market players

Faith in market wisdom
More and better solutions in future

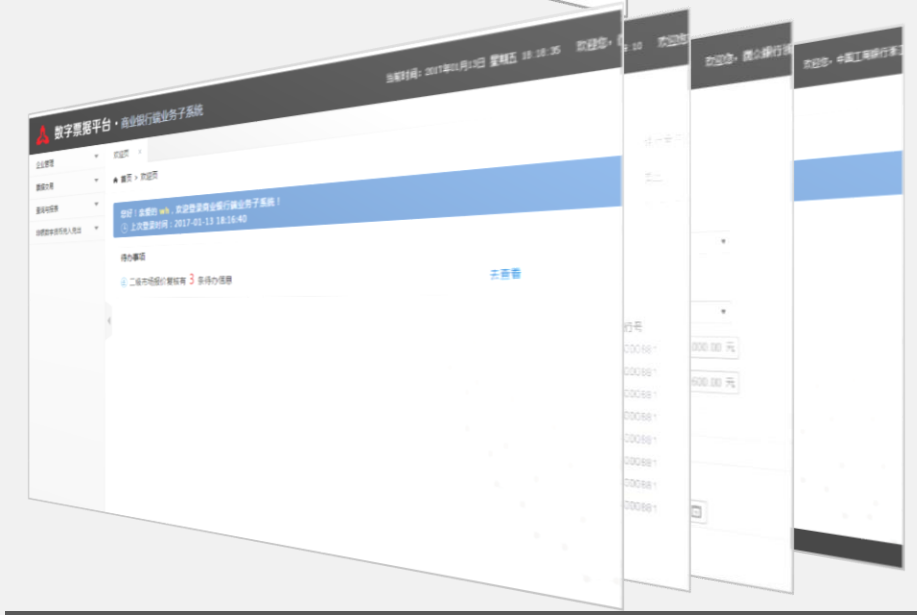
VI

2.DFC IDM1.0 experiment

中国人民银行
THE PEOPLE'S BANK OF CHINA

Central bank system

Interconnection
of
all parties



Commercial bank systems

Digital commercial paper system

VI

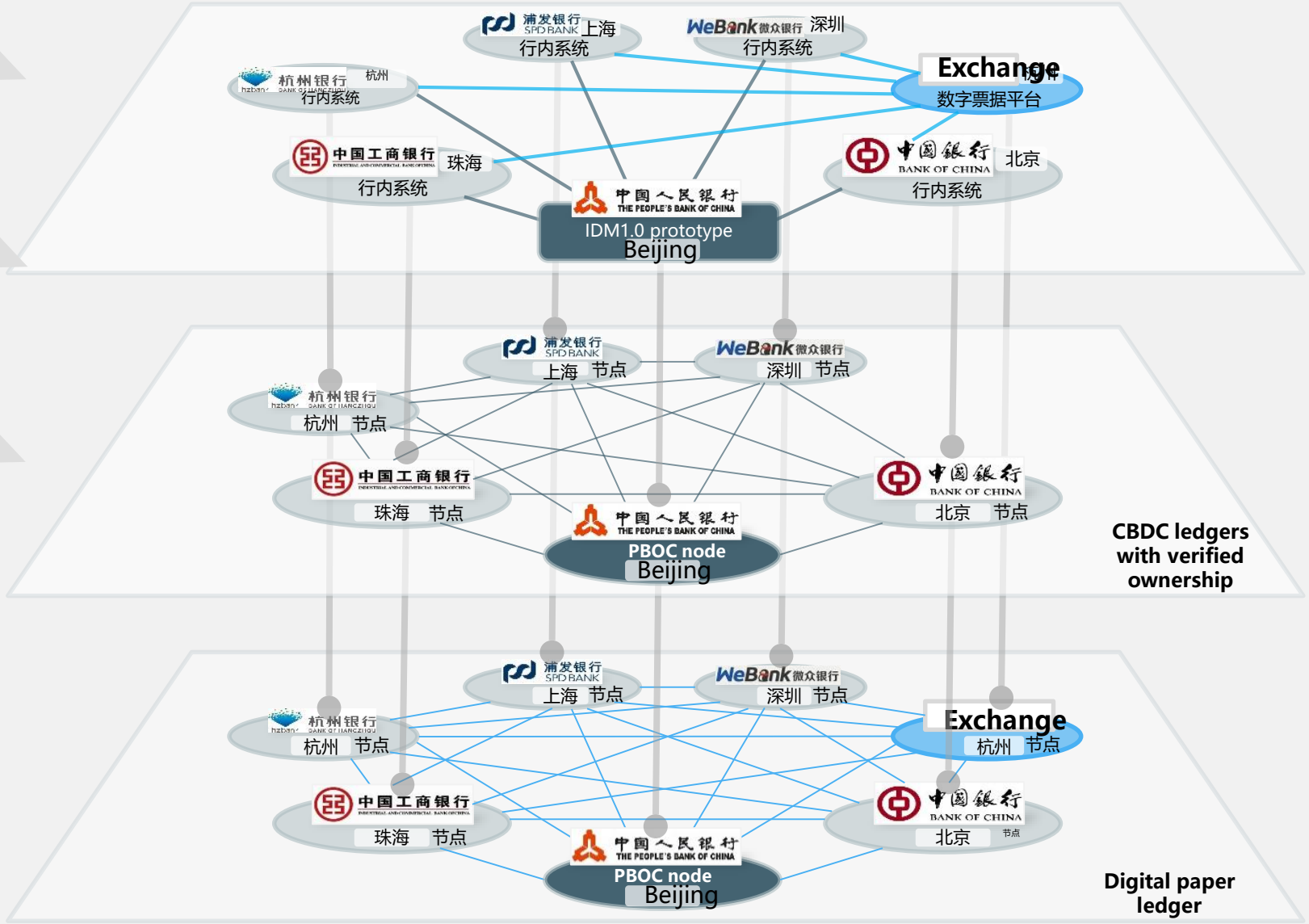
2.DFC IDM1.0 experiment

中国人民银行
THE PEOPLE'S BANK OF CHINA

PBOC & 5 commercial banks

Digital commercial paper platform of Shanghai Commercial Paper Exchange

Full participation of PBOC and banks in system development & connections



Intra net

Outer net

3.Comments review

CHINA ECONOMIC REVIEW

Charting China's changing economic terrain

Since 1990

Latest | Business | Economics & Policy | Columns & Interviews | Markets & Finance | House View

PBOC moves closer to issuing digital currency

Thursday, January 26, 2017

Share:

The People's Bank of China (PBOC) completed a successful trial run of a digital bank
...k in the world to issue its
...BOC, the central bank on
...ceptance bills using a
...secure digital ledger that

Bloomberg | Quint India's BQ Markets Business Law And Policy Politics

Central Banks Should Lead on Digital Currency, PBOC's Fan Says

by Bloomberg News

Updated on September 5, 2016, 4:01 pm
Published on September 2, 2016, 11:24 am

(Bloomberg) -- People's Bank of China Vice Governor Fan Yifei said the monetary authority is pushing to supervise private digital currencies and develop its own digital money.

The PBOC should also consider how to maintain financial stability, innovation, and proper supervision on the issuance and circulation of its legal digital tender, Fan, who leads the central bank's cryptocurrency research, wrote in a Bloomberg View guest column Friday. Sensible rules and macroprudential controls should guide that development, Fan said.

"With internet access increasing and encryption technology improving, the conditions are ripe for digital currencies, which can reduce operating costs, increase efficiency and enable a wide range of new applications," Fan wrote.

Fan's commentary on the the fast-changing world of digital currency suggests policy makers in Beijing want to take the lead in researching and developing digital currencies. PBOC Governor Zhou Xiaochuan said earlier this year digital currency will co-exist with cash for quite a long time before it eventually replaces cash.

PBOC: the first to research on CBDC and is leading studies worldwide

2014 **Preliminary exploration**

Study on physical cash, difference between non-cash payment instruments and digital currency, implementation technologies and management. Produced a series of feasibility reports on digital currency.

2015 **Deeper studies**

More manpower to research team. Expand scope of studies to incorporate general framework of digital currency, technologies & standards, legal issues, application environment, impact of digital currency on monetary policy and financial stability, impact on issuance and international experience. Produced a set of reports covering multiple dimensions.

2016 **Specialized studies and experiments**

Jan — PBOC digital currency seminar held in Beijing which identified the goal of PBOC to issue digital currency

By Sept — Apply a series of patents. Released articles on digital currency at China Finance. Established Institute of Digital Money.

Year-end — Developed PBOC DFC experimental system to be applied in digital commercial paper trading scenario.

The world's first DFC experiment genuinely participated by central bank and commercial banks.

MIT Technology Review

2017/01/23

https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency/

Intelligent Machines

China's Central Bank Has Begun Cautiously Testing a Digital Currency

The People's Bank of China has developed a digital currency that's designed to scale to the number of transactions made every day across the country.

by Will Knight June 23, 2017

Is not the only country interested in overhauling its currency. This year India eliminated some banknotes in an effort to reduce tax evasion and illegal income. And while some other central banks, including the Bank of England, the Bank of Canada, Deutsche Bundesbank, and the Monetary Authority of Singapore, are studying digital fiat currencies,

China's test appears to be the first of its kind anywhere in the world.

One of the main concerns voiced by other central banks looking at digital fiat currencies is that they could undermine the commercial

3.Comments review

Caixin Vol 24, 2017

"

Just before the Spring Festival of 2017,

The experiment on the DLT-based prototype for digital commercial paper trading was successfully tested. It could be connected to digital currency prototype system, and key underlying technologies were all developed by PBOC.

The success is attributable to cooperation between PBOC and many institutions including ICBC, BOC, SPD Bank, Hangzhou Bank and WeBank.

Triggered high attention to PBOC's efforts in CBDC studies from home and abroad.

"

81 patent applications filed to the State Intellectual Property Office

By June 2018

5.Market-driven competition & pick the best

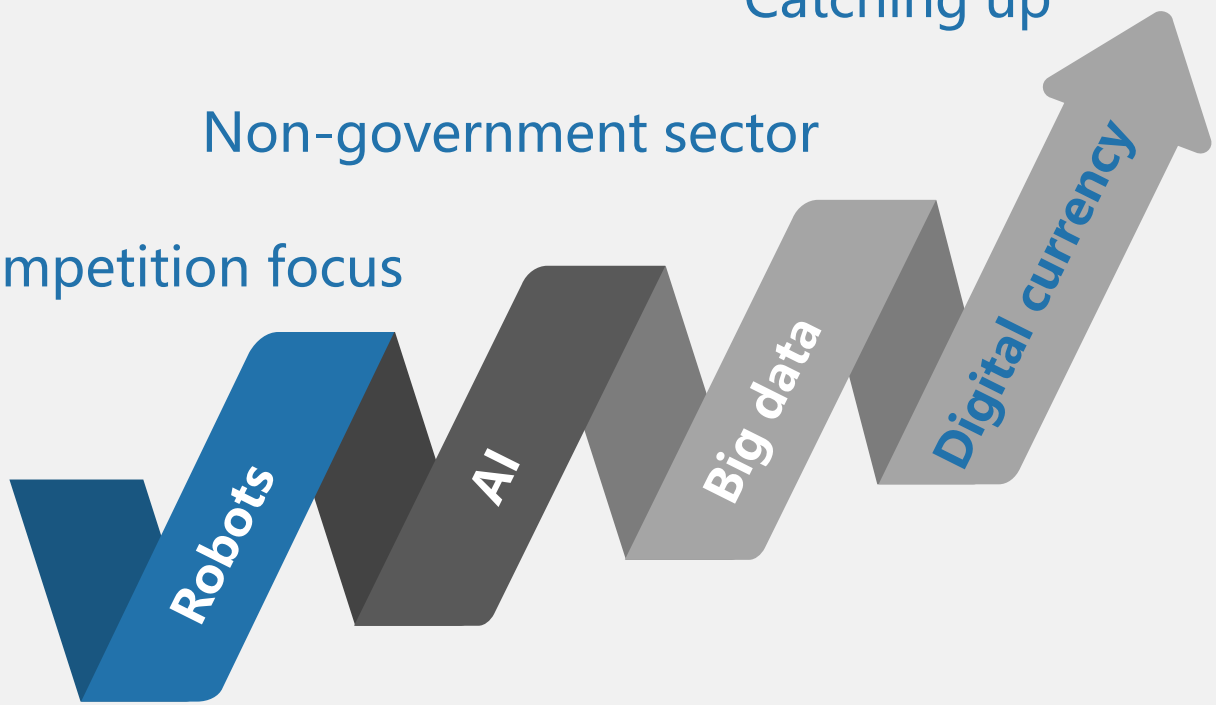
The Economist

Critical significance

Catching up

Non-government sector

Competition focus



中国人民银行
THE PEOPLE'S BANK OF CHINA

THANKS

谢　谢　聆　听

中国人民银行数字货币研究所