Technical Aspects of CBDC in a Two-Tiered System

YAO Qian

Institute of Digital Money,
People’s Bank of China
Central banks of major economies devoted to research on digital currency

**Bank of England**
- 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

- Coinage technology: No fake, higher value stability, higher data security, stronger regulation, more flexible payment, more effective control measures.
- Value support: Better service to the public, foundation of RegTech.
3. Four dimensions of CBDC

Electronic money + Physical cash = CBDC

Value: Credit-based currency
Technical: crypto-currency
Implementation: algorithm-based currency
Application: Smart currency
4. Design principle of CBDC system

**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
1. Evolution of traditional binary system

**Chinese DFC: Theories and Architecture**

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

**DFC: Theories and Architecture**

- Incentives to banks
- Participation of banks
- Proper diversification of risks
- Accelerate service innovation

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
Two-tiered system
Central bank – Commercial banks

Currency system

Least shock

Business architecture

Infrastructure

Users

Application 1

Application ...

Application n

Obtain / Recycle

Circulate
## 3. Business framework in a two-tiered system

### Business framework

<table>
<thead>
<tr>
<th>Central bank</th>
<th>Commercia l bank</th>
<th>End users</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issue</strong></td>
<td><strong>Circulate</strong></td>
<td><strong>Retrieve</strong></td>
</tr>
<tr>
<td>Issue</td>
<td>Ownership verification</td>
<td>Retrieve</td>
</tr>
<tr>
<td>Register</td>
<td>Transfer registration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authorization mgt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ownership verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transfer registration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authorization mgt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ownership verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transfer registration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authorization mgt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ownership verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transfer registration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authorization mgt</td>
<td></td>
</tr>
<tr>
<td><strong>Manage &amp; Control</strong></td>
<td><strong>Retrieve</strong></td>
<td><strong>Manage &amp; Control</strong></td>
</tr>
<tr>
<td></td>
<td>AML</td>
<td>Risk mgt</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Inter-connection</td>
</tr>
<tr>
<td></td>
<td>Risk mgt</td>
<td>Data analysis</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>KYC</td>
</tr>
</tbody>
</table>

- **Issue**
  - Issue
  - Register

- **Circulate**
  - Ownership verification
  - Transfer registration
  - Authorization mgt

- **Retrieve**
  - Retrieve

- **Manage & Control**
  - AML
  - Risk mgt
  - Audit
  - Security
  - Inter-connection
  - Data analysis

- **End users**
  - Deposit & withdraw
  - Pay

- **User mgt**
  - Operation

- **Error response**
  - Error response

- **Wallet**
  - Log in
  - Wallet
Design principle

Two-tiered system

Form of presentation

Controlled anonymity

Smart contract

Realization of design concept
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.

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

PBOC proposed an encrypted DFC solution.

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

JP Koning proposed the FedCoin and provided solution for retail payment.
2. Loose-coupling ①: Loosely coupled with bank accounts in terms of form

Centralized issuance

Account-based loose coupling

- Easy to circulate
- Controlled anonymity

CBDC

Variable length

Programmable script

Variable length

Issuer signature

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

An implementation model: based on commercial bank account

- Commercial bank
- Issuing bank
- Business/Individual
- Commercial bank account system
- Digital currency wallet
- Physical currency
- ¥ E-currency
- ¥ Digital currency
- Deposit/Withdraw

Digital currency
- Ownership of digital currency verified by agents
- Greatly enhance KYC and AML capacity of banks

Traditional bank accounts
CONTENTS

01  Design principle
02  Two-tiered system
03  Form of presentation
04  Controlled anonymity
05  Smart contract
06  Realization of design concept
1. Protect privacy of information owners via institutional arrangements

**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

- Protect information owners
- Managed by regulators
- Demands
- Used by various types of institutions
2. Find optimal equilibrium for privacy protection

Utility of financial service consumers vs. Privacy protection

Optimal equilibrium

- 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

Utility of financial institutions

Privacy protection

- Consumer information stolen
- Financial institutions’ reputation impaired
- Higher operation costs and application for financial institutions

Optimal equilibrium
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.

**Proper disclosure of financial information**

<table>
<thead>
<tr>
<th>Identity info</th>
<th>Financial trading info</th>
<th>Derivative info</th>
<th>Info access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Trading elements</td>
<td>Trading scenarios</td>
<td></td>
</tr>
<tr>
<td>Central bank</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Counterparty</td>
<td>○</td>
<td>•</td>
<td>○</td>
</tr>
<tr>
<td>Agents</td>
<td>○</td>
<td>•</td>
<td>○</td>
</tr>
<tr>
<td>Commercial bank</td>
<td>•</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

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

- Accessible info
- Inaccessible info
- Partially accessible info
1. Two types of smart contract

**Executable script embedded in digital currency**

- **Executable script**
  - Programs saved as plain text
  - Similar to natural language
  - Facilitate rapid development & control

**System-dependent smart contract**

- **Smart contract**—a set of commitments defined in digital form
  - Data inputs
    - Incidents inputs
      - Pre-defined response conditions
      - Pre-defined response conditions
  - Action 1
  - Action n

- **Contract status**
  - Contract value

- **Automatic**
  - **Permanent operation**
  - **Real-time**
  - **Cost-effective**
  - **Time efficient**
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

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

**CBDC**
CONTENTS

01 Design principle
02 Two-tiered system
03 Form of presentation
04 Controlled anonymity
05 Smart contract
06 Realization of design concept
1. 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
2.0FC IDMI.D experiment

Central bank system

Interconnection of all parties

Commercial bank systems

Digital commercial paper system
2. DFC IDM1.0 experiment

PBOC & 5 commercial banks

Digital commercial paper platform of Shanghai Commercial Paper Exchange

Full participation of PBOC and banks in system development & connections

CBDC ledgers with verified ownership

Intra net

Outer net

Digital paper ledger
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


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.
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 inoverhauling 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
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. Just before the Spring Festival of 2017, 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

Digital currency

AI

Big data

Robots
THANKS

谢谢聆听

中国人民银行数字货币研究所