Stablecoins and Central Bank Digital Currency

Neha Narula
Director, Digital Currency Initiative
Massachusetts Institute of Technology
MIT’s Digital Currency Initiative

Mission

Empower people by making it as easy to move value as it is to move information

Values

- User agency
- Open source
- Rigor

Approach

Decentralized networks and centralized digital currency. Neutral technology research & development; not involved in token sales

Timeline

- 2015: Founded in the Media Lab to support Bitcoin
- 2016: First CBDC hire
- Disclosed major bug in Bitcoin Cash
- 2018: Recruited Gary Gensler as Senior Advisor
- Addressed major inflation bug in Bitcoin
- 2020: Began collaboration with FRBB on CBDC
Problems

- **High fees**: Retail transaction costs comprise 0.5-0.9% of GDP (depending on the country)
- **Lack of access**: 7.1 million American households don’t have bank account
- **Slow and inefficient**: Stimulus checks took 5 months
- **Stability**: Concerns with growth in private payment options
- **Lack of innovation**: Comparison to Asian payment platforms

### Public and private forms of money and payments

**Money**:
- **Public**: Cash, Central bank reserves
- **Private**: Bank deposits, E-money, Stable-coins

**Payments**:
- **Public**: Cash, Electronic bank transfers
- **Private**: E-money payment platforms, Credit cards, Checks, Debit cards
Today’s solutions try to build interoperability after-the-fact and face significant barriers:

- **Disparate systems:** each sub-system (vendor) has unique technical protocols (e.g., data models, payment protocols, identity management), risk tolerances, incentives, and regulatory schemes

- **Misaligned stakeholders:** existing stakeholders have vested interests in the system (e.g., maintaining rents more important than improving access and tech)
How might stablecoins or CBDC help?

- Improve efficiency and costs by improving competition and streamlining digital payment rails
- Improve accessibility for financial inclusion
- Provide more auditability and insight into the economy
- Potential for innovation from smart contracts
Do stablecoins and CBDCs compete?

Yes and no

- All currencies compete
- Overlapping, but also distinct use cases
- Stablecoins and CBDC can coexist
- A lot depends on design and regulation
Range of proposals for innovating in payments and retail central bank digital currency

1. Give more institutions access to CB accounts
2. Stablecoins
3. “Synthetic” CBDC
4. Two-tier CBDC (requires commercial bank account)

Retail CBDC definition
- Liability of the central bank
- Held and transferred digitally
- Accessible to the general public (also called GPCBDC)
Stablecoin risks

- Solvency
- Liquidity
- Fraud
- Illicit activity
- Operation and technology
Stablecoin operation and technology risks

- Underlying blockchain (security, fees)
- Stablecoin smart contract
- Minting and redemption process
- How to address blockchain/stablecoin provider disagreements

Range of proposals for innovating in payments and retail central bank digital currency

1. Give more institutions access to CB accounts
2. Stablecoins
3. “Synthetic” CBDC
4. Two-tier CBDC (requires commercial bank account)
5. Give individuals access to CB accounts
6. Digital cash
7. CB issues tokens on a public blockchain
## CBDC landscape

### Actors and stakeholders
- Central Banks and governments
- Commercial banks
- Large tech companies
- Fintech (e-money providers)
- Telecoms
- Blockchain companies

### What is not being addressed
- Neutral rigorous research
- Assessing impact of technical options on users (especially the poor)
- Advanced policy discussions
- Crisp, coherent definitions and frameworks
<table>
<thead>
<tr>
<th>Source</th>
<th>Commonly referred to as “token”</th>
<th>Commonly referred to as “account”</th>
<th>Intended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kahn 2016</td>
<td>Bearer instrument (possession)</td>
<td>Custodial (identification of person)</td>
<td>Ownership and authentication</td>
</tr>
<tr>
<td>Auer and Böhme 2020</td>
<td>Authenticated via digital signature</td>
<td>Authenticated via identity credentials</td>
<td>Authentication</td>
</tr>
<tr>
<td>Armelius et al 2021</td>
<td>Sequence of bits</td>
<td></td>
<td>Digital object</td>
</tr>
<tr>
<td>Chaum et al 2021</td>
<td>Value and issuer</td>
<td>Transaction history</td>
<td>History</td>
</tr>
<tr>
<td>Computer Scientists</td>
<td>UTXOs (destroy/create)</td>
<td>Balances (increment/decrement)</td>
<td>Data model</td>
</tr>
<tr>
<td>Source</td>
<td>Commonly referred to as “token”</td>
<td>Commonly referred to as “account”</td>
<td>Intended meaning</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Kahn 2016</td>
<td>Bearer instrument (possession)</td>
<td>Custodial (identification of person)</td>
<td>Ownership and authentication</td>
</tr>
<tr>
<td>Auer and Böhme 2020</td>
<td>Authenticated via digital signature</td>
<td>Authenticated via identity credentials</td>
<td>Authentication</td>
</tr>
<tr>
<td>Armelius et al 2021</td>
<td>Sequence of bits</td>
<td>Transaction history</td>
<td>Digital object</td>
</tr>
<tr>
<td>Chaum et al 2021</td>
<td>Value and issuer</td>
<td>Transaction history</td>
<td>History</td>
</tr>
<tr>
<td>Computer Scientists</td>
<td>UTXOs (destroy/create)</td>
<td>Balances (increment/decrement)</td>
<td>Data model</td>
</tr>
<tr>
<td>Other</td>
<td>Transfers are final</td>
<td>Transfers are reversible</td>
<td>Settlement</td>
</tr>
<tr>
<td></td>
<td>P2P</td>
<td>Requires an intermediary</td>
<td>Transfer intermediation</td>
</tr>
<tr>
<td></td>
<td>Smart contracts</td>
<td>APIs</td>
<td>Interface</td>
</tr>
<tr>
<td></td>
<td>DLT</td>
<td>Database</td>
<td>Architecture</td>
</tr>
<tr>
<td></td>
<td>Anyone can use</td>
<td>Must register and sign up</td>
<td>Access</td>
</tr>
<tr>
<td></td>
<td>Single tier</td>
<td>Two tier</td>
<td>Distribution</td>
</tr>
<tr>
<td></td>
<td>Anonymous</td>
<td>Requires identity</td>
<td>Identification</td>
</tr>
<tr>
<td></td>
<td>Data not shared or stored in plain text</td>
<td>Data shared with CB or intermediaries</td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td>Doesn’t required network connectivity</td>
<td>Requires network connectivity</td>
<td>Offline capability</td>
</tr>
<tr>
<td></td>
<td>Operates 24/7</td>
<td>Operates during business hours</td>
<td>Availability</td>
</tr>
</tbody>
</table>
Example: transfer intermediation

- **P2P**
- **Cash**
- **Cryptocurrency**

Requires an intermediary

- **Bank transfers**
Intermediation is not a binary choice

- Small cash transactions
- $10K+ cash transactions
- Bank transfers

- Bitcoin
  - Requires miners to accept transaction
- USDC
  - Funds can be frozen
- Enforced legally
  - Bitcoin through an exchange
  - Funds can be frozen
Range of proposals for innovating in payments and retail central bank digital currency

Existing system

1. Give more institutions access to CB accounts
2. Stablecoins
3. “Synthetic” CBDC

New

4. Two-tier CBDC (requires commercial bank account)
   - Give individuals access to CB accounts
   - Digital cash
5. CB issues tokens on a public blockchain
Potential to redefine financial roles and introduce new players

Key roles

- CBDC issuance, redemption, and distribution
- Wallet set-up and maintainence
- User authentication and KYC
- Transaction authorization
- Transaction validation
- Transaction settlement
- Data analysis
Don’t start the design conversation with the technology

- What are the policy goals?
- How should it work as money?
- How should it be accessed?
- What is the desired market structure?
- What are acceptable data retention and privacy policies?
- What are the hoped-for policy tools?
However, technical CBDC research is still vital

**Foundational technical research needed…**

- **Policy goals and choices under consideration**, but feasibility still unknown

- **Technical designs impact long-term policy outcomes** (e.g., internet protocols defined today’s market structure)

- **Circuitous, wasteful debate on false design choices** (e.g., token vs account, DLT vs traditional database)

**…and it’s critical to start with the core transaction processing engine**

- Basic feasibility and baseline performance needed before new and complex features can be tested

- Core transaction processing engine becomes a research platform for future experimentation

* There’s no point designing the seat before the plane
Project Hamilton: Build an at-scale and flexible retail transaction processing research framework

Research collaboration between the Federal Reserve Bank of Boston and MIT

Meet 4 key retail CBDC requirements

- **Throughput** – over 100K tx/sec
- **Latency** – finality in <5 sec
- **Resiliency** – No single points of failure
- **Security** – Minimize attack surface

And create a **flexible** platform for experimentation and collaboration

- Enable different design options
  - e.g. self-hosted wallets, strong privacy, intermediary roles
- Support innovative features
  - e.g. programmability, interoperability, cross-border, offline payments
CBDCs can only achieve their potential if we engage in multi-disciplinary research today

Initial MIT DCI CBDC research areas (non-exhaustive)

1. High performance architectures
2. Privacy and compliance
3. Usability
4. Roles, innovation, and incentives
5. Offline access
6. Programmability
7. Policy tools
Summary

● Stablecoins and CBDC represent an opportunity for a ground-up redesign of payments infrastructure; each comes with risks and benefits
● Oversimplified CBDC technical choices have hijacked economist and policymaker attention
● Achieving CBDC’s potential will require deep collaborative work between technologists, economists, and policymakers