



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

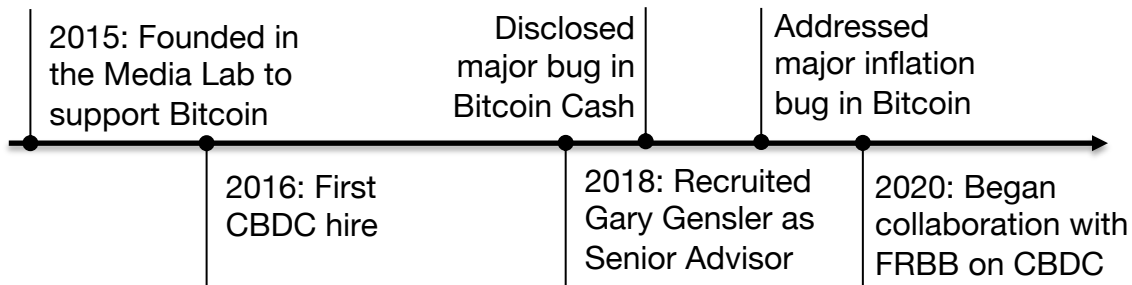


Approach

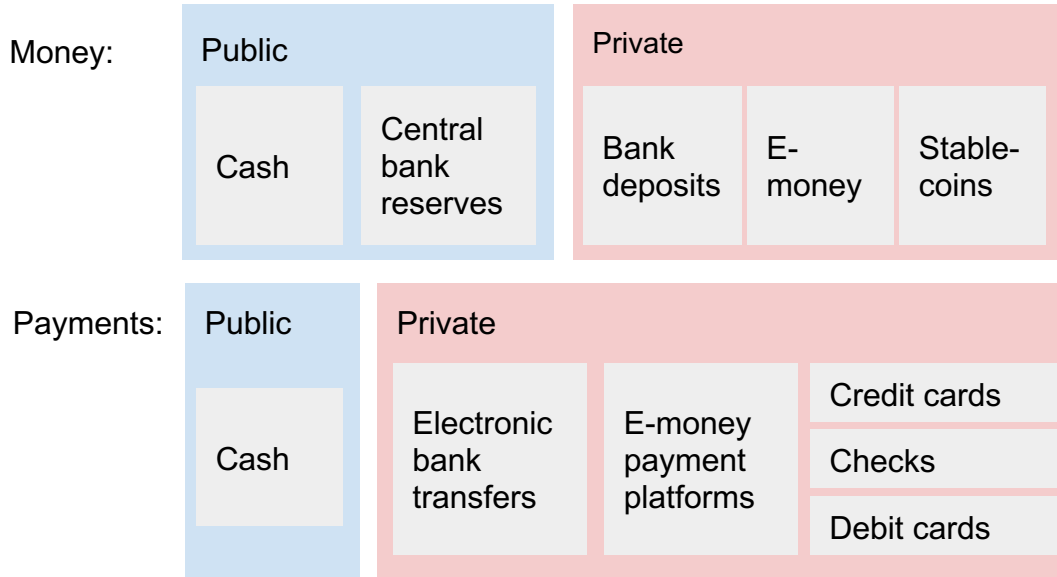
Decentralized networks and centralized digital currency. Neutral technology research & development; not involved in token sales



Timeline



Public and private forms of money and payments



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

Existing solutions have had limited impact

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 2 3 4

Give more institutions access to CB accounts Stablecoins “Synthetic” CBDC

Two-tier CBDC (requires commercial bank account)



Give individuals access to CB accounts Digital cash CB issues tokens on a public blockchain

6 7

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

Stablecoin risks

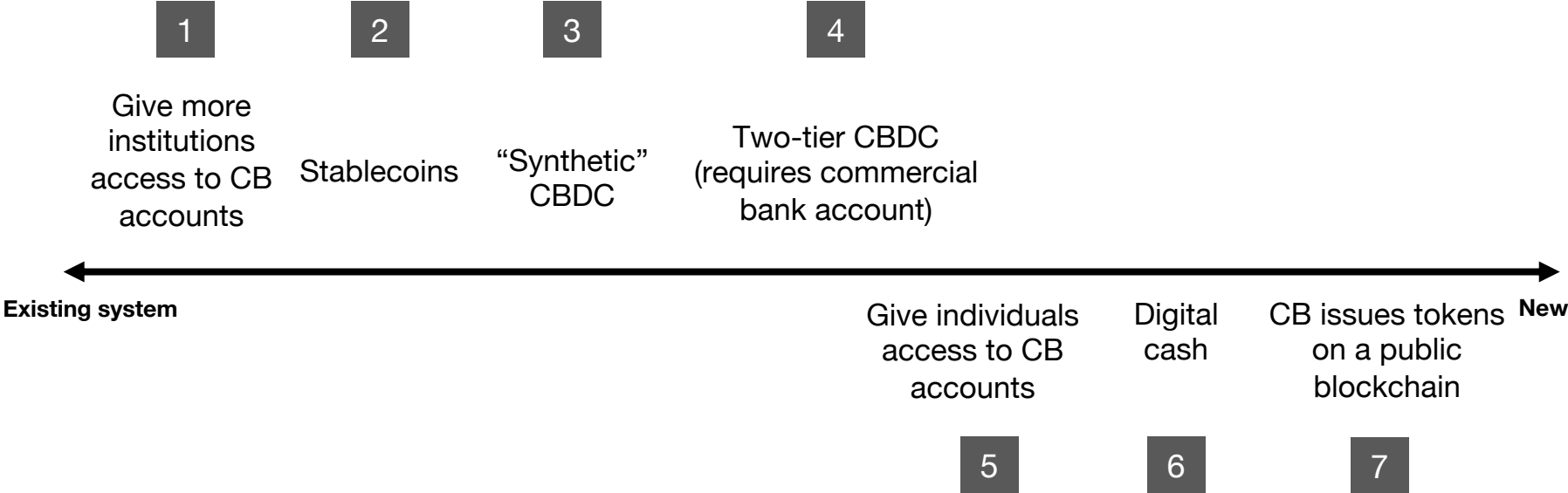
- Solvency
- Liquidity
- Fraud
- Illicit activity
- **Operation and technology**

Stablecoin operation and technology risks

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

<https://nehanarula.org/2021/09/23/stablecoins.html>

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



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

Source	Commonly referred to as “token”	Commonly referred to as “account”	Intended meaning
Kahn 2016	Bearer instrument (possession)	Custodial (identification of person)	Ownership and authentication
Auer and Böhme 2020	Authenticated via digital signature	Authenticated via identity credentials	Authentication
Armelius et al 2021	Sequence of bits		Digital object
Chaum et al 2021	Value and issuer	Transaction history	History
Computer Scientists	UTXOs (destroy/create)	Balances (increment/decrement)	Data model

Source	Commonly referred to as “token”	Commonly referred to as “account”	Intended meaning
Kahn 2016	Bearer instrument (possession)	Custodial (identification of person)	Ownership and authentication
Auer and Böhme 2020	Authenticated via digital signature	Authenticated via identity credentials	Authentication
Armelius et al 2021	Sequence of bits		Digital object
Chaum et al 2021	Value and issuer	Transaction history	History
Computer Scientists	UTXOs (destroy/create)	Balances (increment/decrement)	Data model
Other	Transfers are final	Transfers are reversible	Settlement
	P2P	Requires an intermediary	Transfer intermediation
	Smart contracts	APIs	Interface
	DLT	Database	Architecture
	Anyone can use	Must register and sign up	Access
	Single tier	Two tier	Distribution
	Anonymous	Requires identity	Identification
	Data not shared or stored in plain text	Data shared with CB or intermediaries	Privacy
	Doesn't required network connectivity	Requires network connectivity	Offline capability
	Operates 24/7	Operates during business hours	Availability

Example: transfer intermediation

P2P

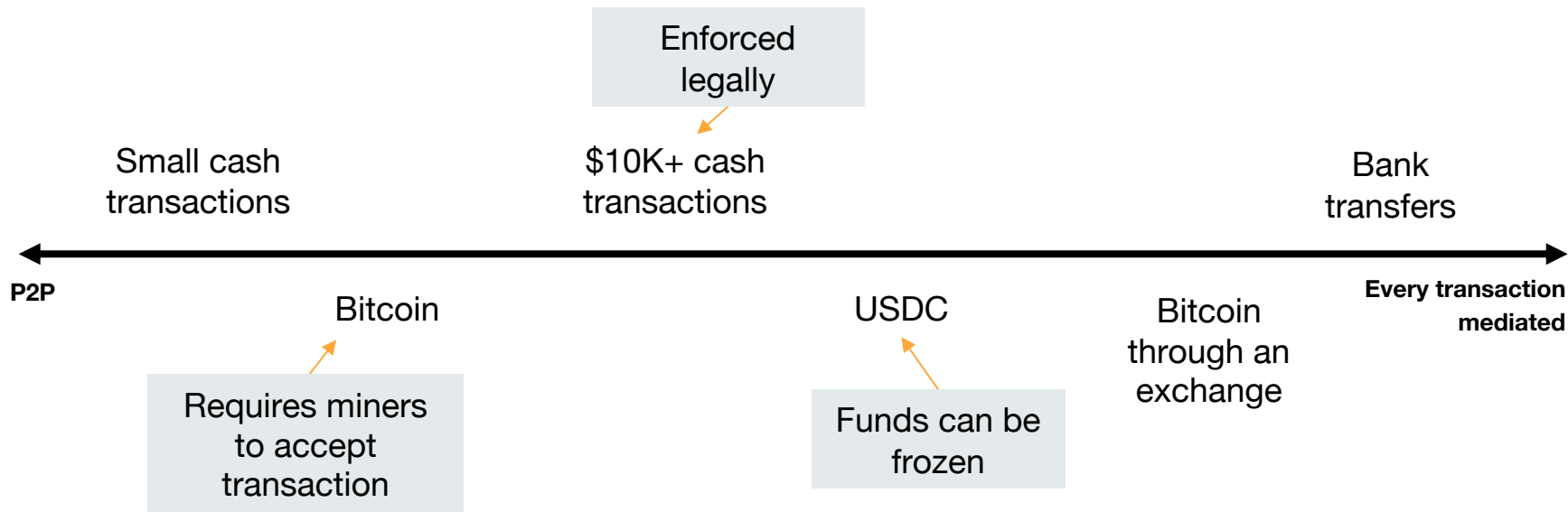
Requires an intermediary

Cash

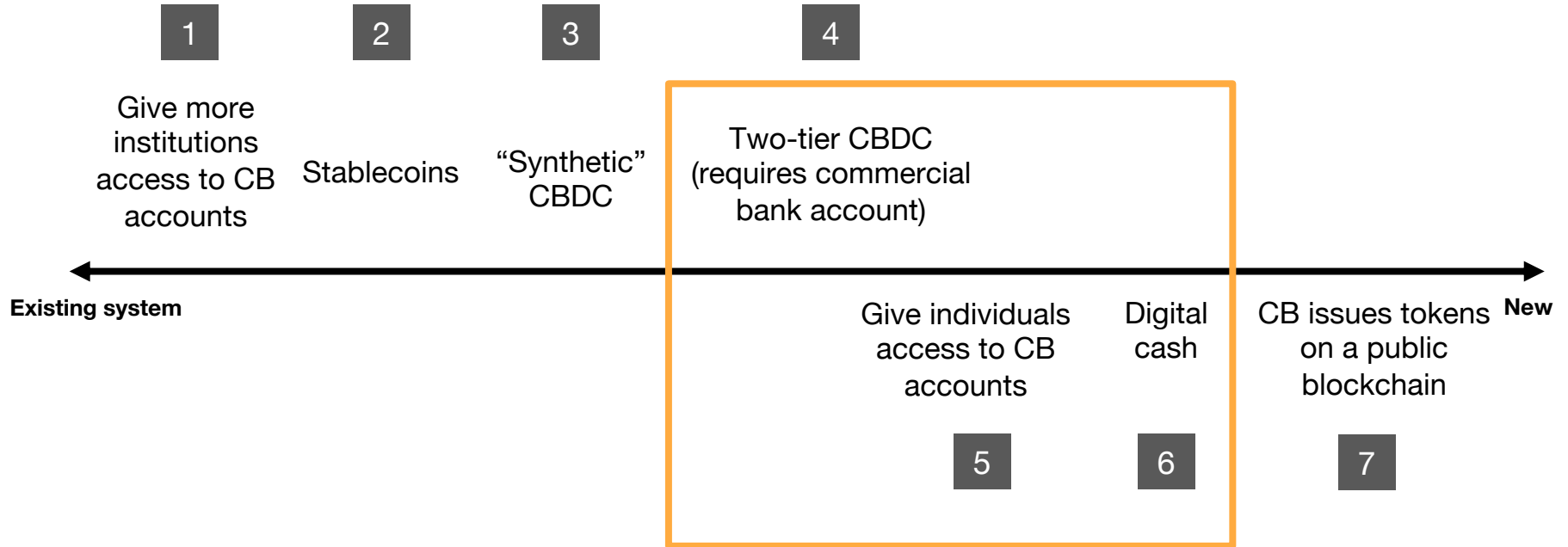
Bank transfers

Cryptocurrency

Intermediation is not a binary choice



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



Potential to redefine financial roles and introduce new players

Key roles

- CBDC issuance, redemption, and distribution
- Wallet set-up and maintenance
- User authentication and KYC
- Transaction authorization
- Transaction validation
- Transaction settlement
- Data analysis



Issuance
Redemption
Ledger maintenance



Digital wallet
management



Identity verification & access
control



Data analysis

Don't start the design conversation with the technology

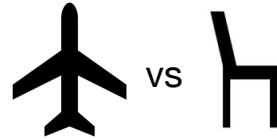
- What are the policy goals?
- How should it work as money?
- How should it be accessed?
- What is the desired market structure?
- What are acceptable data retention and privacy policies?
- What are the hoped-for policy tools?

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



There's no point designing the seat before the plane

- **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

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