# Privacy for Central Bank Digital Currencies

Jeremy Clark

MADIBA security research group

UNIVERSITÉ Concordia UNIVERSITY

GINA CODY SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

# FUNDING & PARTNERS:

NSERC CRSNG

Raymond Chabot Grant Thornton

catallaxy

AUTORITÉ DES MARCHÉS FINANCIERS

Fonds de recherche Nature et technologies Québec

Office of the Privacy Commissioner of Canada

**DIDEM DEMIRAG, CONCORDIA UNIVERSITY**

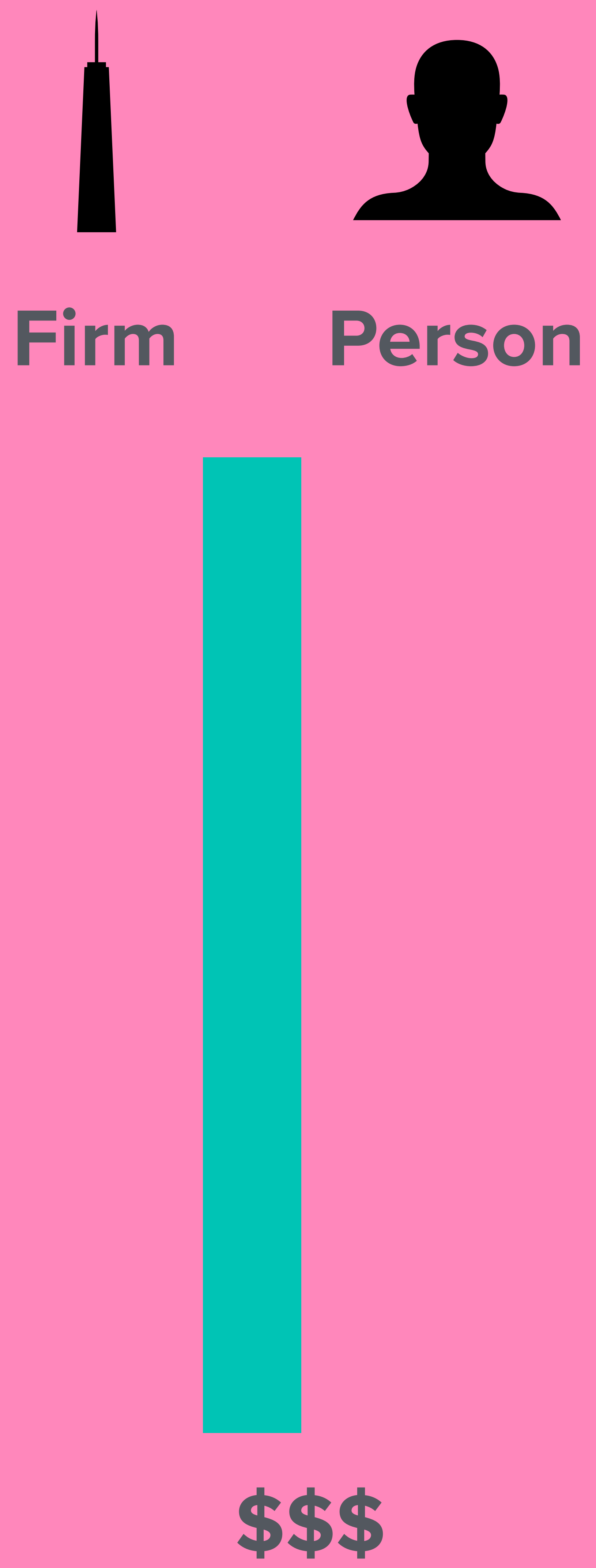
**RAINER BÖHME, UNIVERSITY OF INNSBRUCK**

**RAPHAEL AUER, BANK FOR INTERNATIONAL SETTLEMENTS (BIS)**

**JEREMY CLARK, CONCORDIA UNIVERSITY**

- Central Bank: direct claim (or liability) of the central bank
- Digital Currency: in electronic or digital format

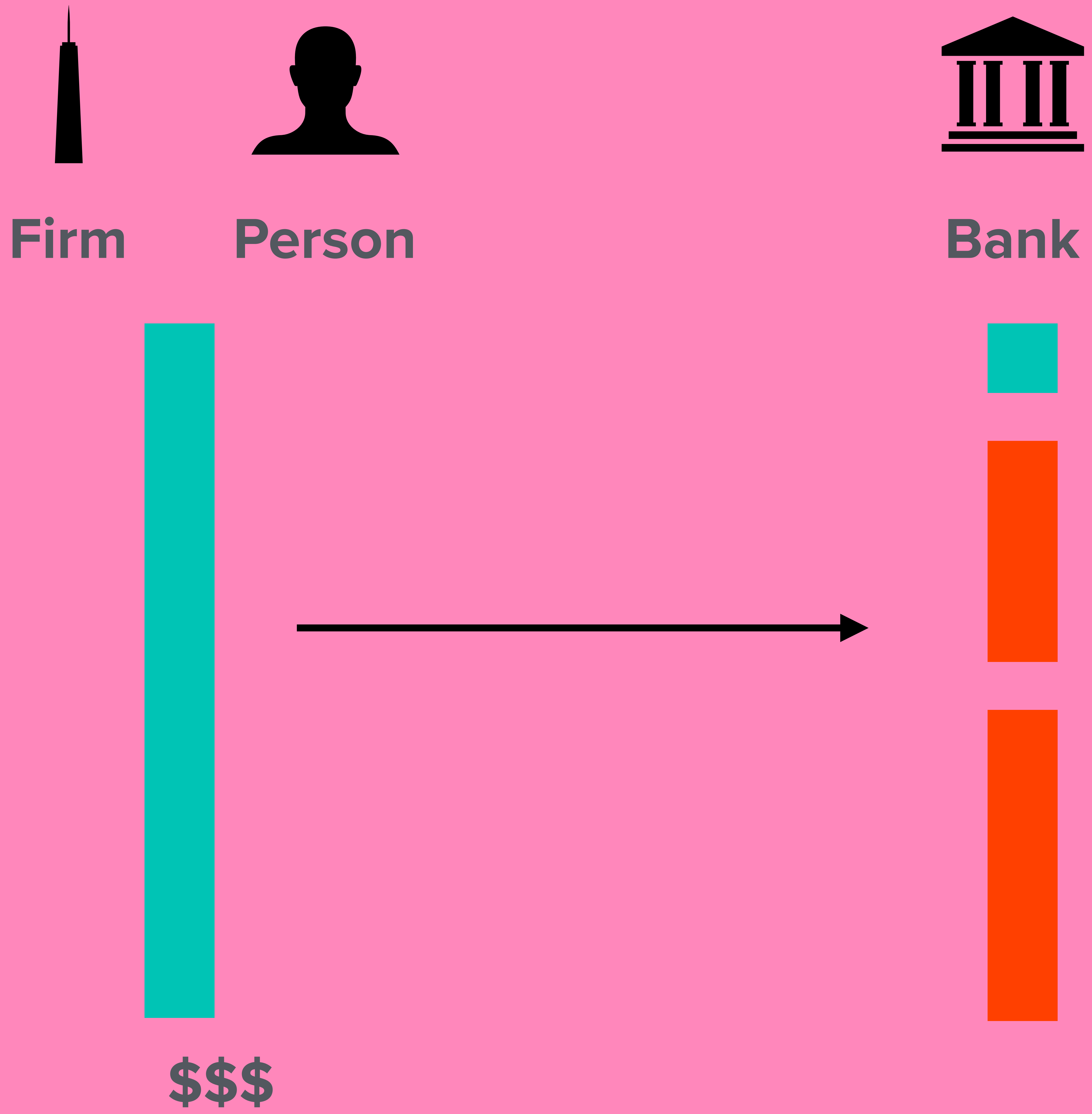
- Central Bank: direct claim (or liability) of *some* central bank
- Digital Currency: in electronic or digital format



Firm

Person

$$$

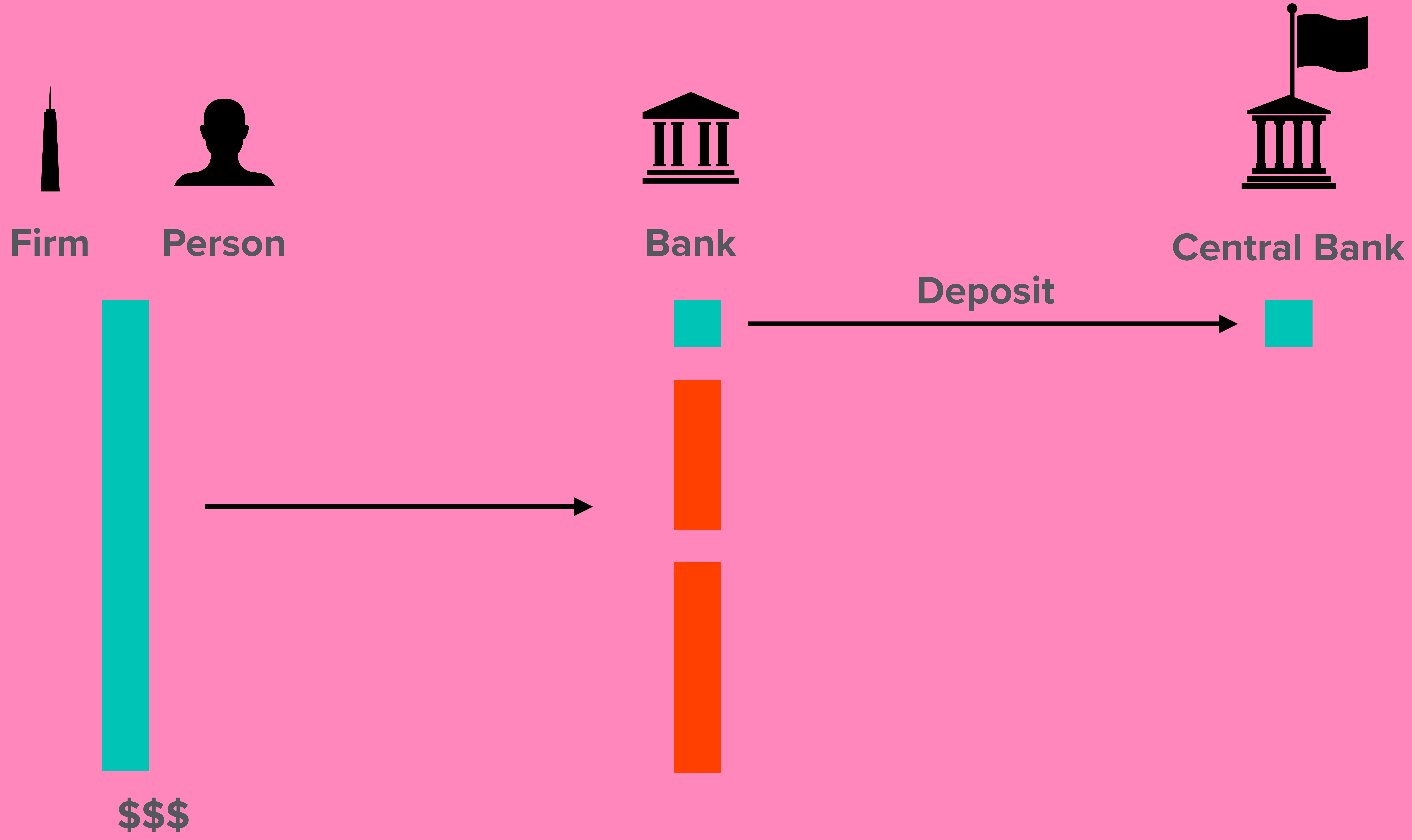


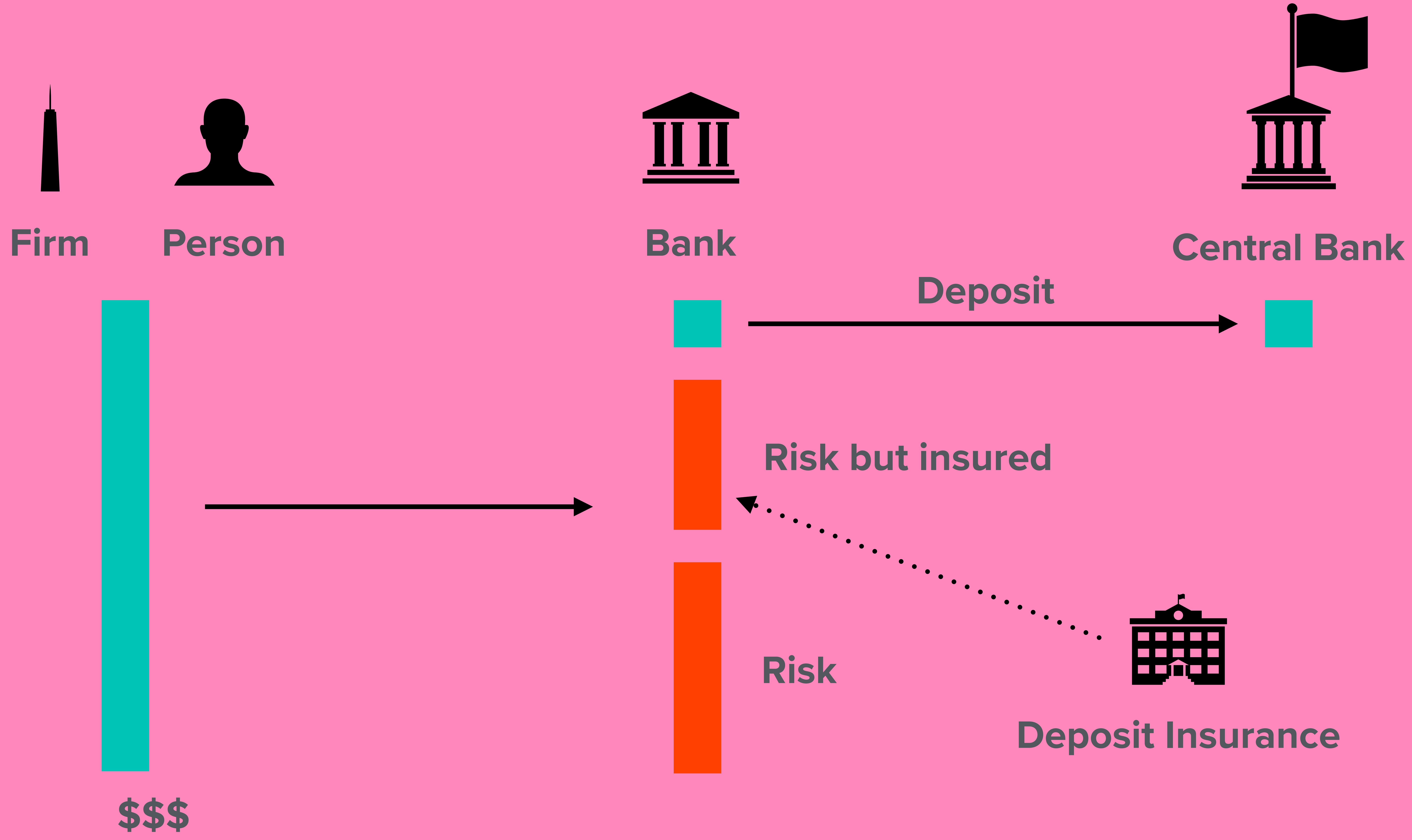
Firm

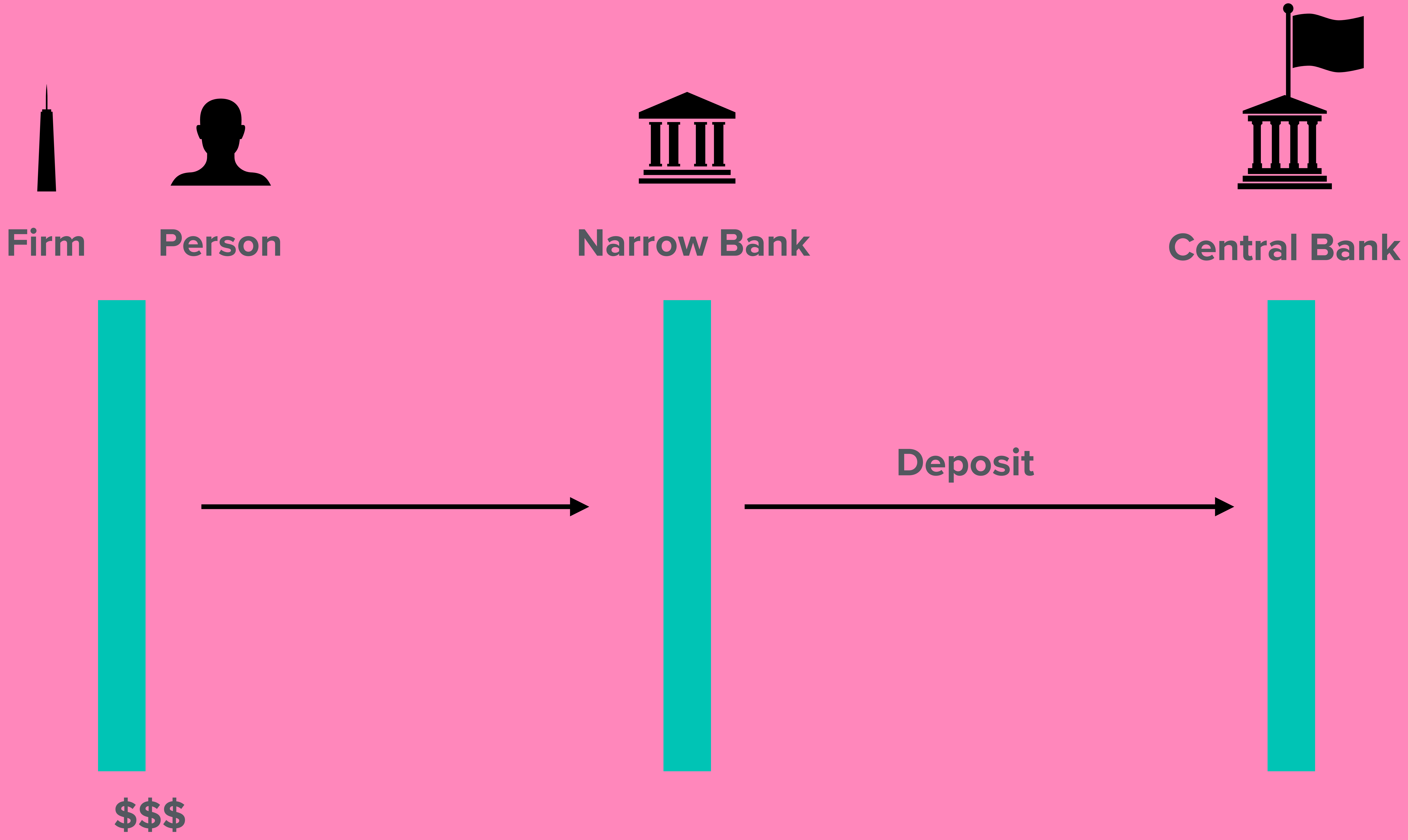
Person

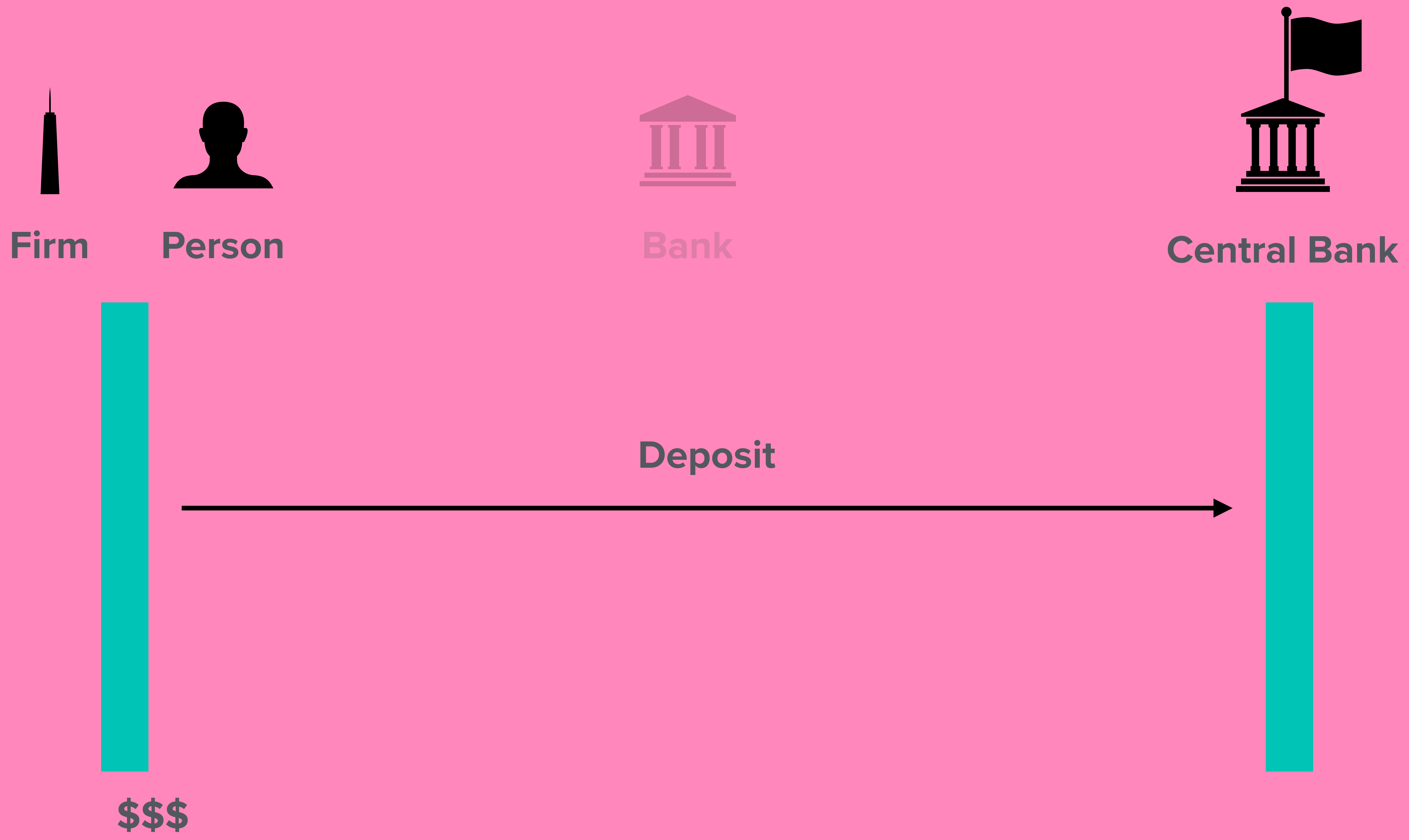
Bank

$$$


Firm
Person
Bank
Central Bank
Deposit
$$$


Firm
Person
Bank
Central Bank
Deposit
Risk but insured
Risk
Deposit Insurance
$$$


Firm
Person
Narrow Bank
Central Bank
Deposit
$$$



Firm

Person

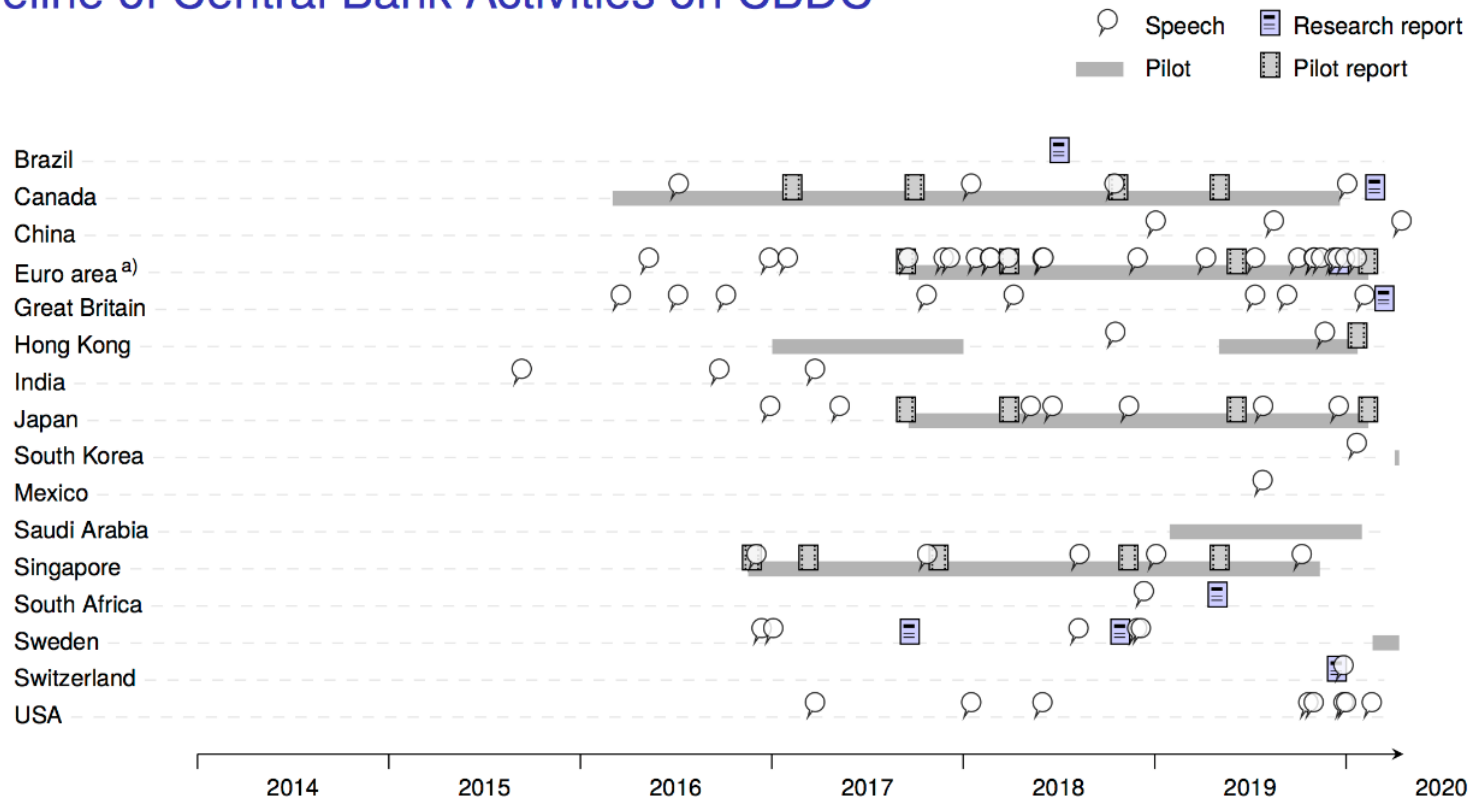
Bank

Central Bank

Deposit

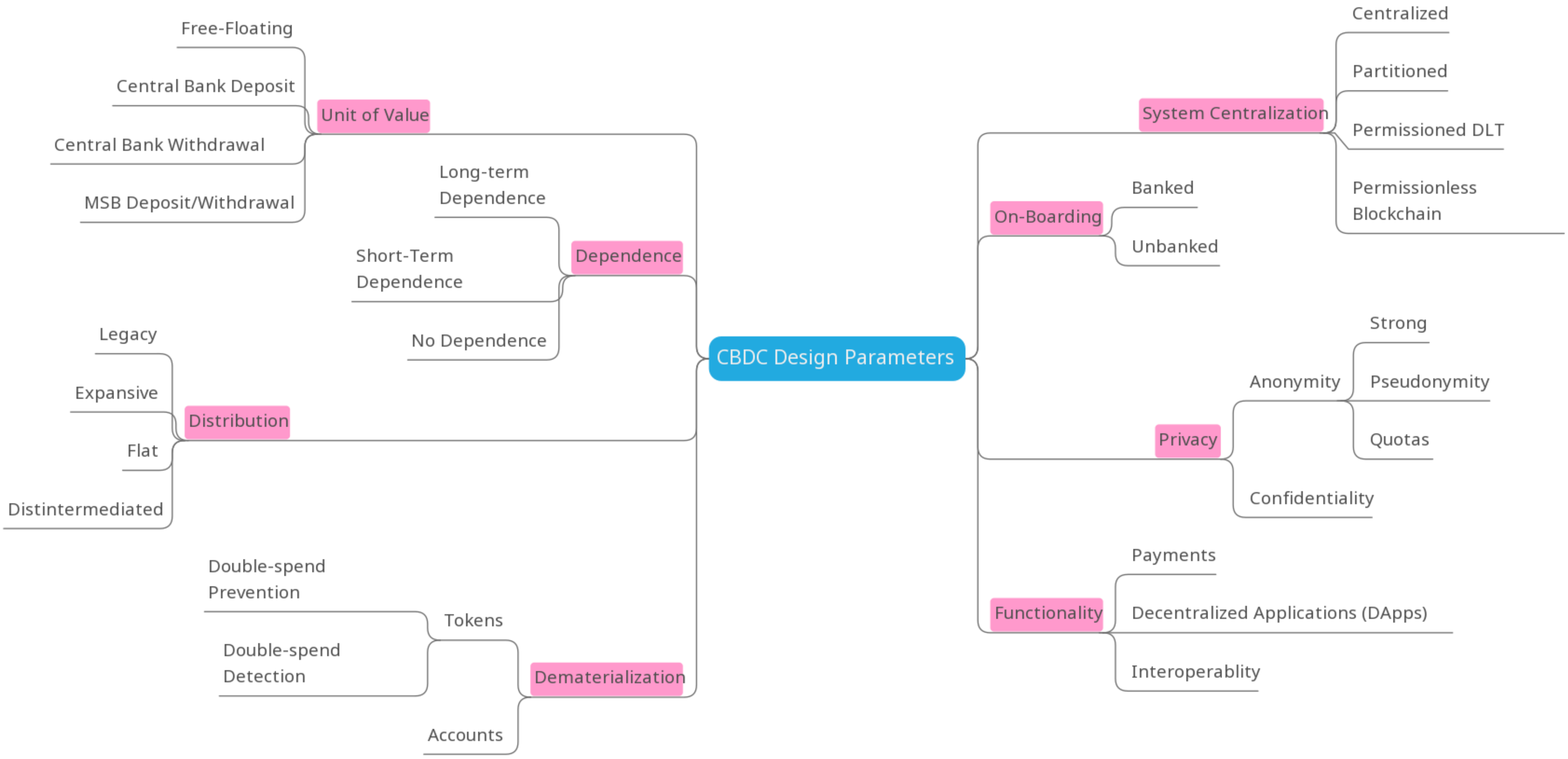
$$$

# Timeline of Central Bank Activities on CBDC



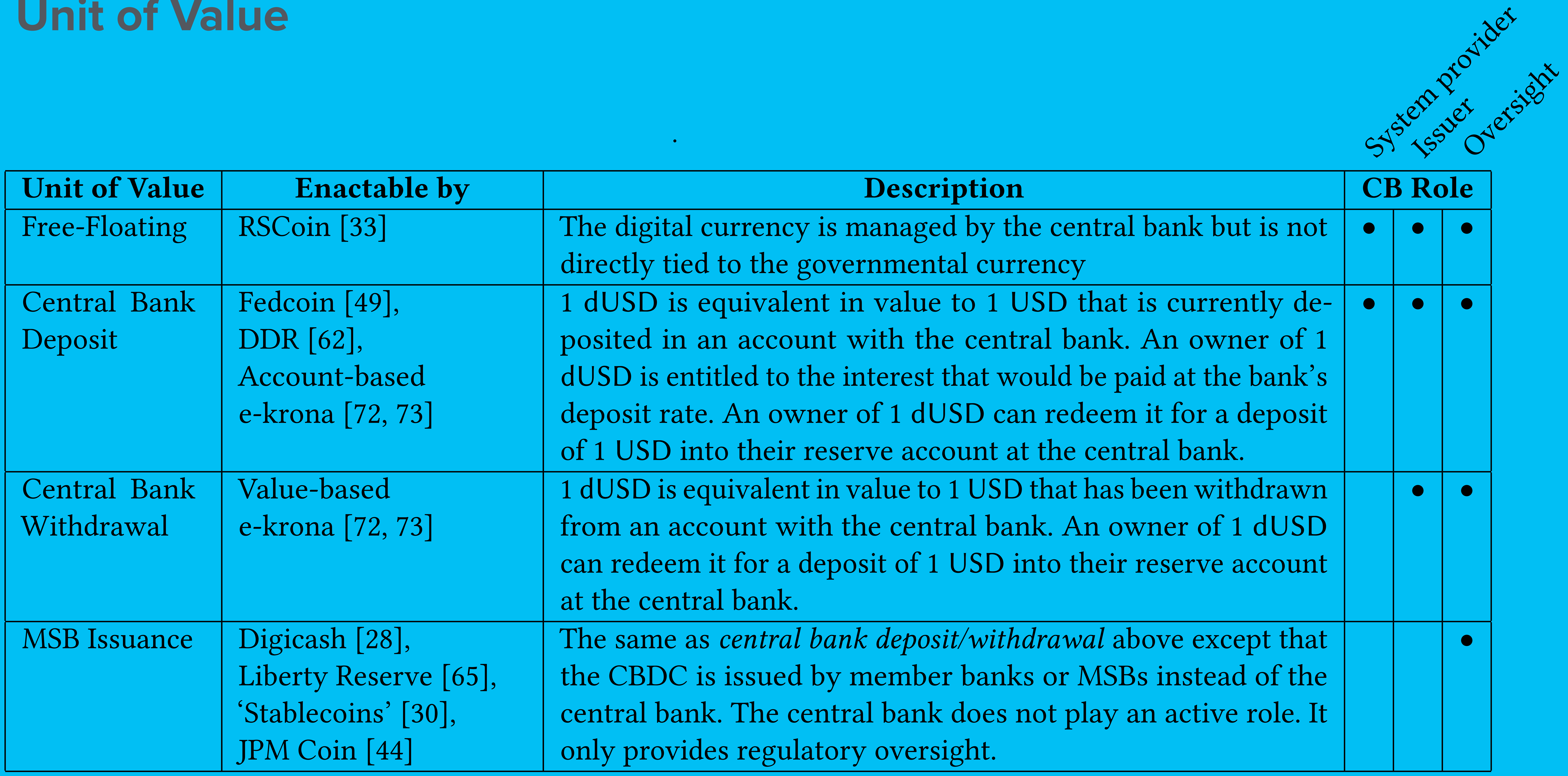
[a)] excluding activities of national central banks within the Eurosystem

Source: Auer et al (2020).

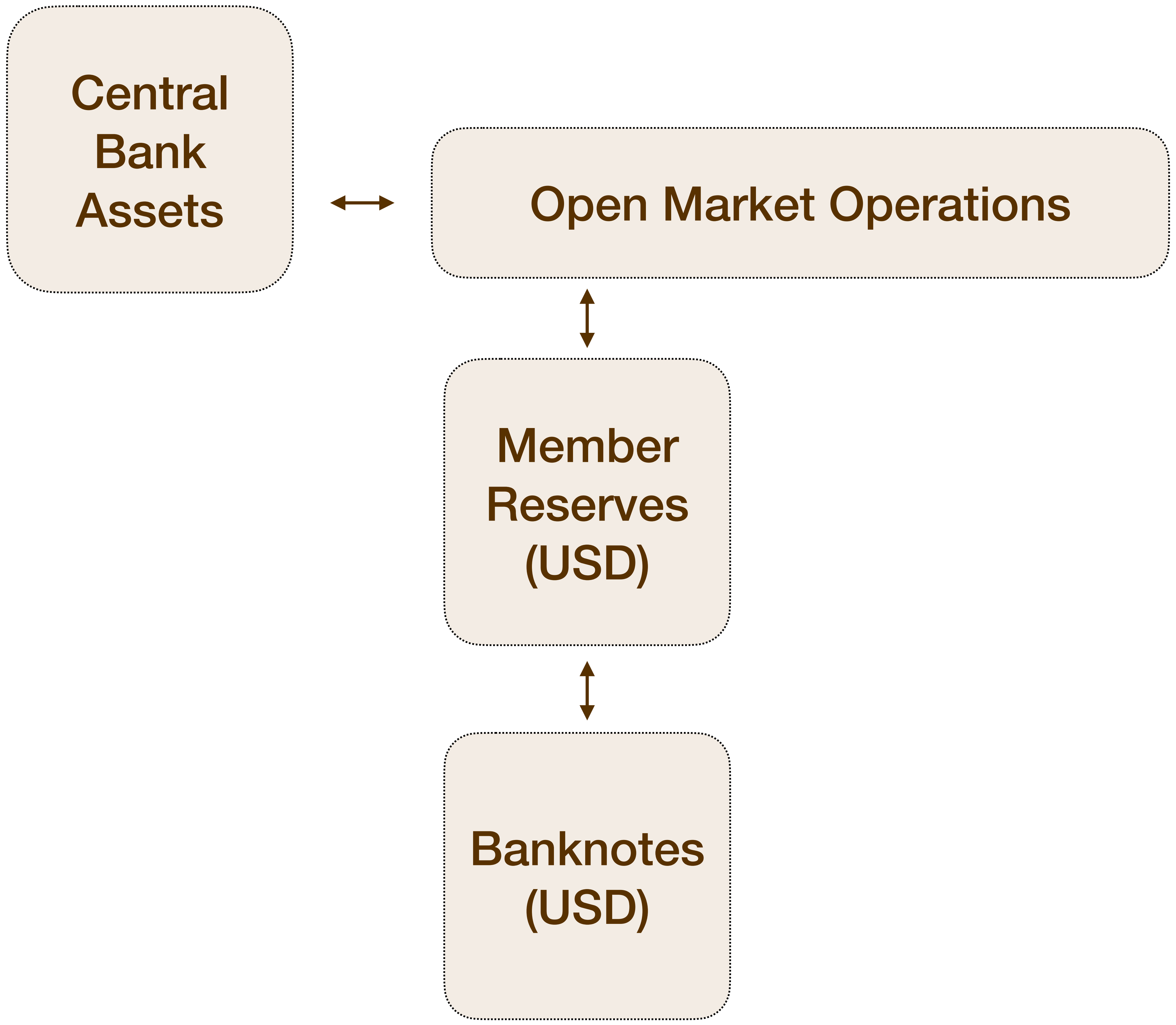


- CBDC Design Parameters
  - Unit of Value
    - Free-Floating
    - Central Bank Deposit
    - Central Bank Withdrawal
    - MSB Deposit/Withdrawal
  - Dependence
    - Long-term Dependence
    - Short-Term Dependence
    - No Dependence
  - Distribution
    - Legacy
    - Expansive
    - Flat
    - Distintermediated
  - Dematerialization
    - Tokens
      - Double-spend Prevention
      - Double-spend Detection
    - Accounts
  - System Centralization
    - Centralized
    - Partitioned
    - Permissioned DLT
    - Permissionless Blockchain
  - On-Boarding
    - Banked
    - Unbanked
  - Privacy
    - Anonymity
      - Strong
      - Pseudonymity
      - Quotas
    - Confidentiality
  - Functionality
    - Payments
    - Decentralized Applications (DApps)
    - Interoperablity

# Unit of Value



| | | | System provider | Issuer | Oversight |
|---|---|---|---|---|---|
| **Unit of Value** | **Enactable by** | **Description** | **CB Role** | | |
| Free-Floating | RSCoin [33] | The digital currency is managed by the central bank but is not directly tied to the governmental currency | ● | ● | ● |
| Central Bank Deposit | Fedcoin [49],<br>DDR [62],<br>Account-based e-krona [72, 73] | 1 dUSD is equivalent in value to 1 USD that is currently deposited in an account with the central bank. An owner of 1 dUSD is entitled to the interest that would be paid at the bank's deposit rate. An owner of 1 dUSD can redeem it for a deposit of 1 USD into their reserve account at the central bank. | ● | ● | ● |
| Central Bank Withdrawal | Value-based e-krona [72, 73] | 1 dUSD is equivalent in value to 1 USD that has been withdrawn from an account with the central bank. An owner of 1 dUSD can redeem it for a deposit of 1 USD into their reserve account at the central bank. | | ● | ● |
| MSB Issuance | Digicash [28],<br>Liberty Reserve [65],<br>'Stablecoins' [30],<br>JPM Coin [44] | The same as *central bank deposit/withdrawal* above except that the CBDC is issued by member banks or MSBs instead of the central bank. The central bank does not play an active role. It only provides regulatory oversight. | | | ● |

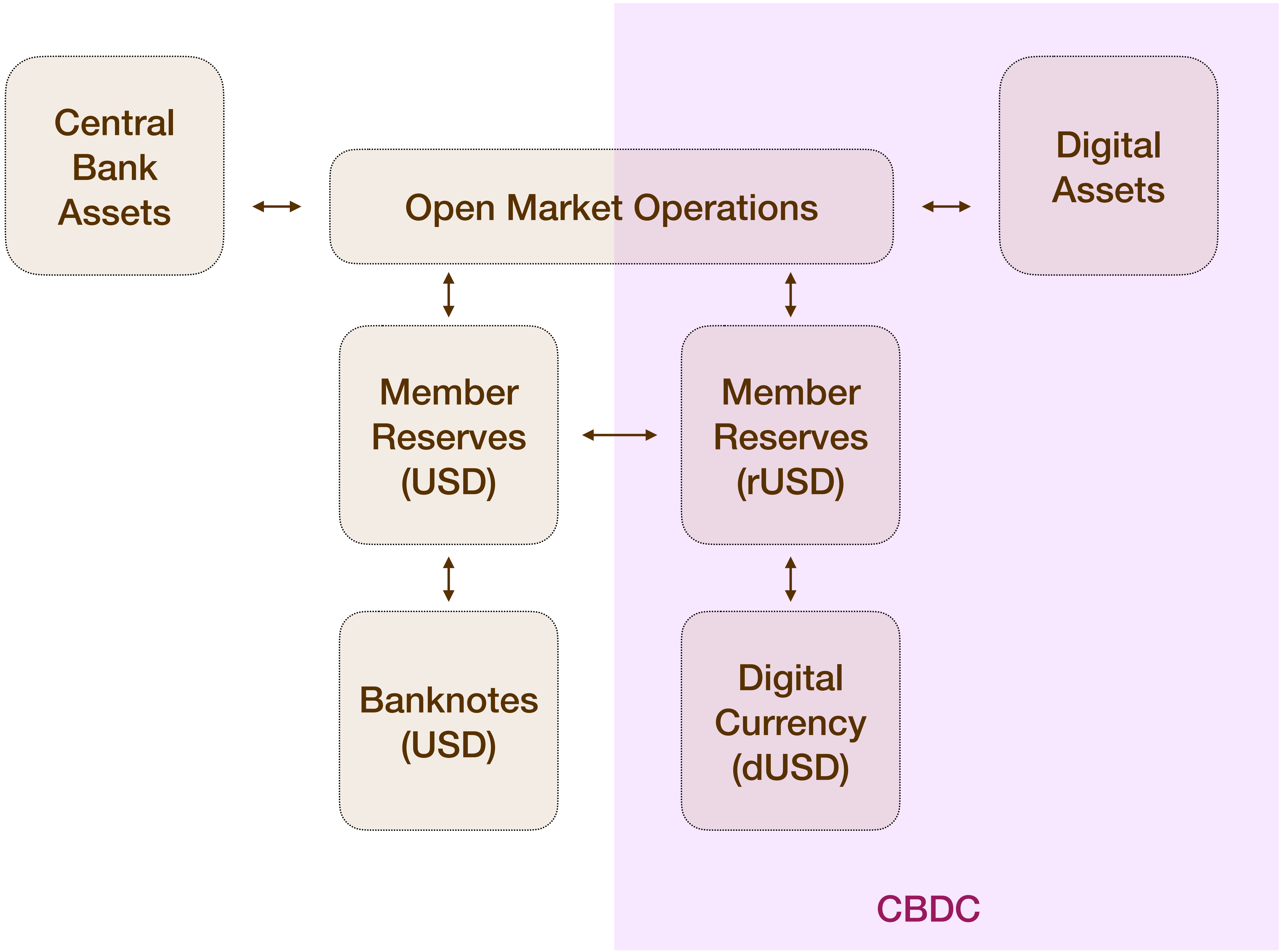


Central Bank Assets

Open Market Operations

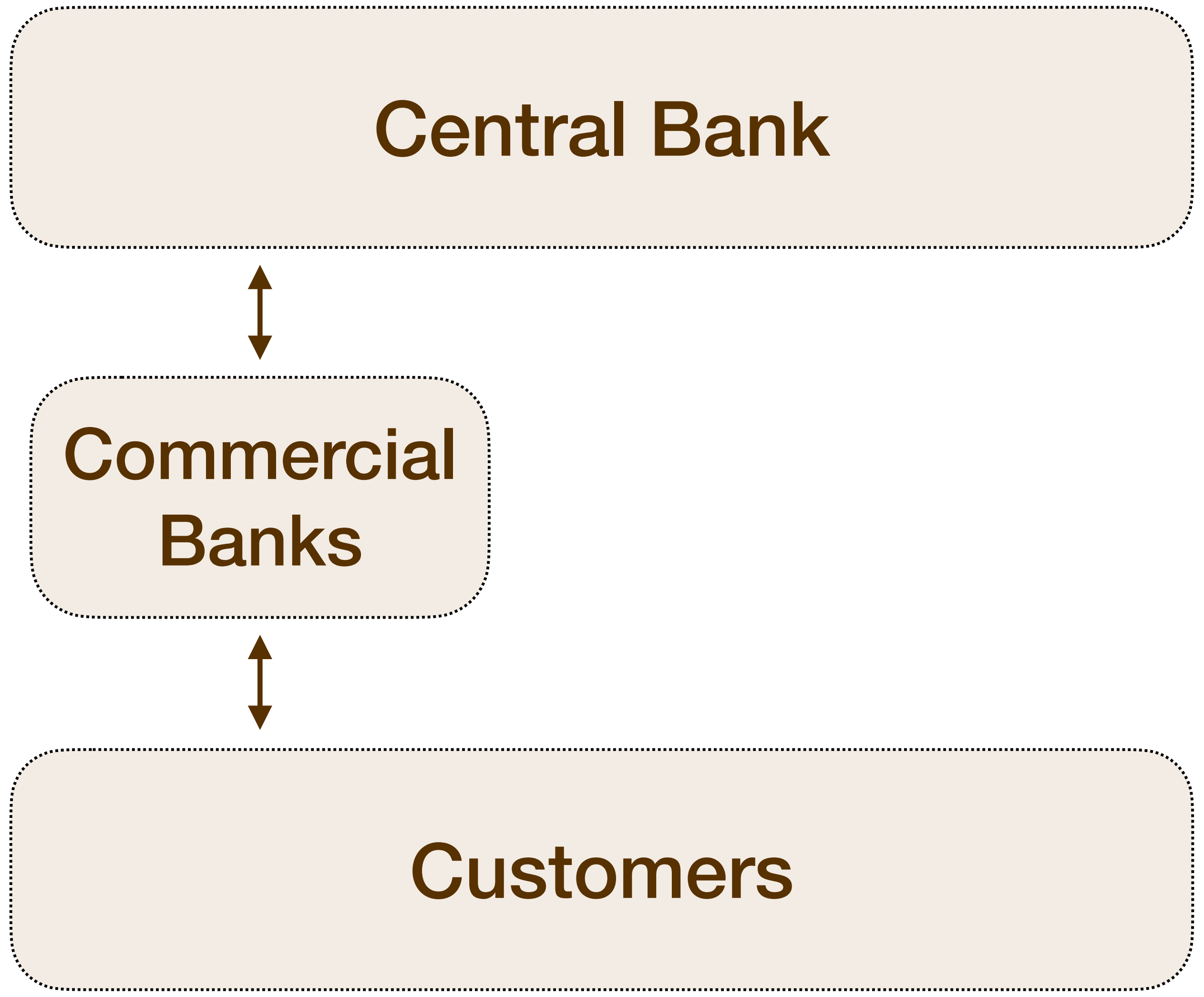
Member Reserves (USD)

Banknotes (USD)


Central Bank Assets
Open Market Operations
Digital Assets
Member Reserves (USD)
Member Reserves (rUSD)
Banknotes (USD)
Digital Currency (dUSD)
CBDC

# Distribution

Legacy/Expansive



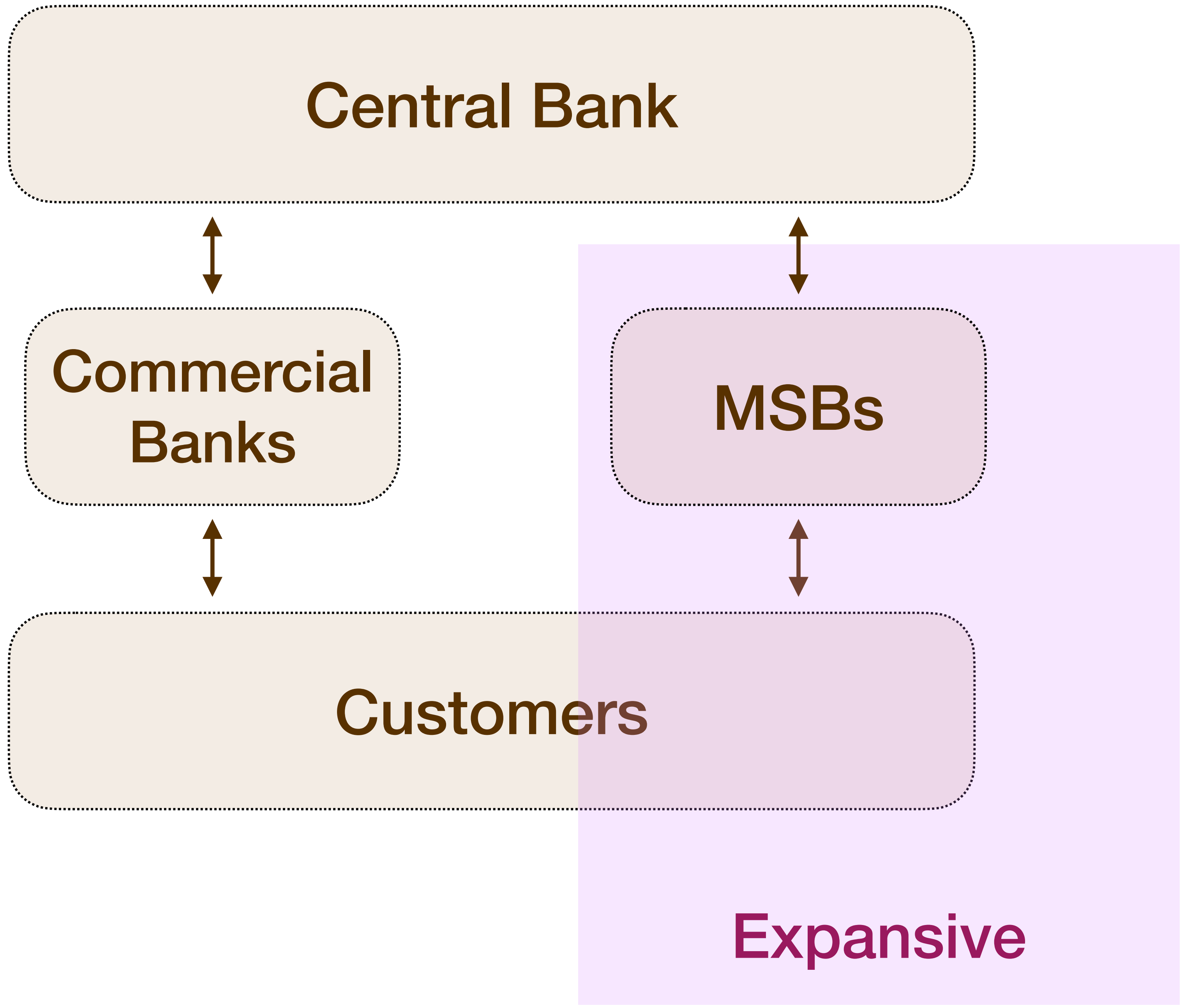
Central Bank

Commercial Banks

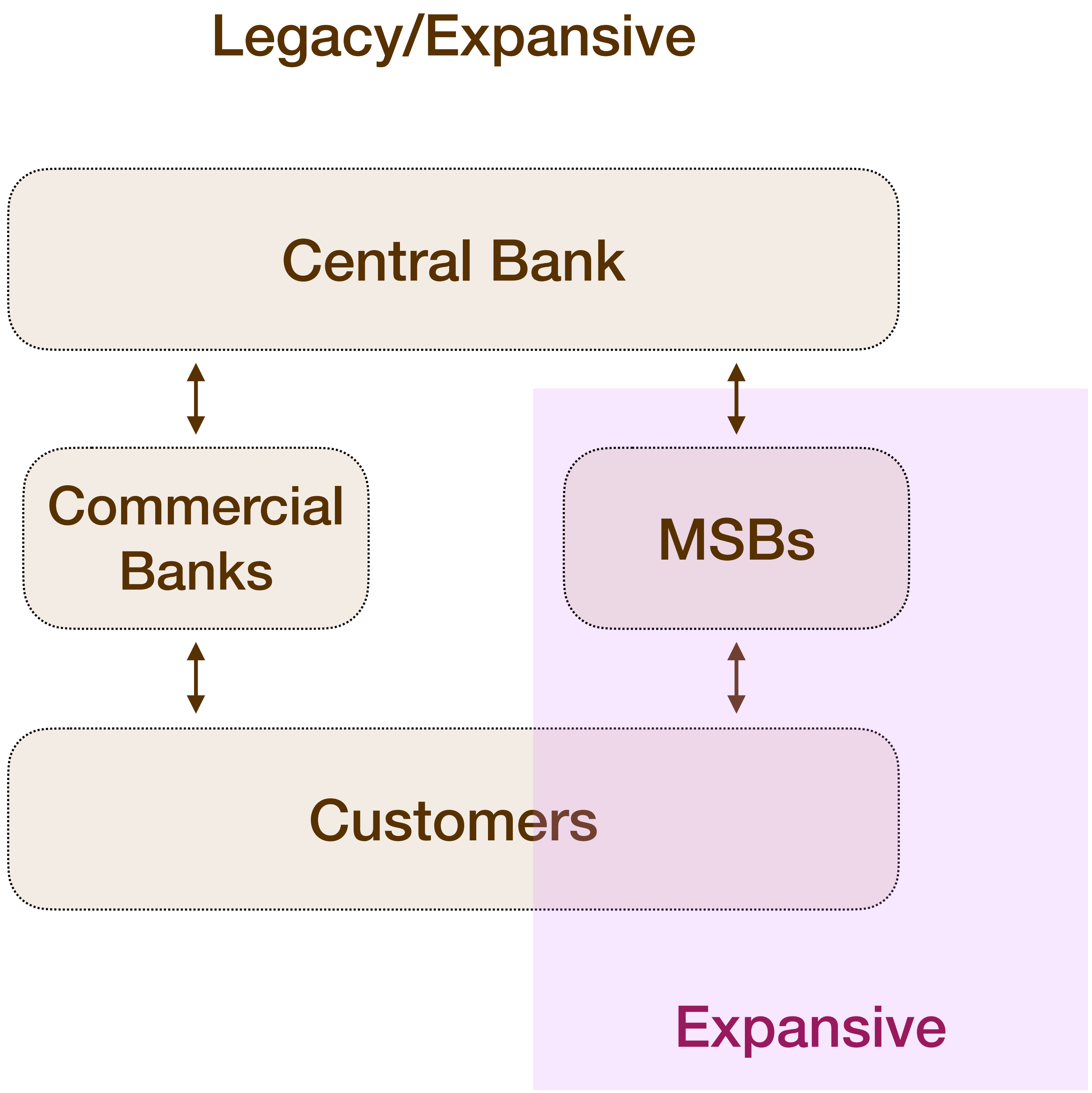
Customers

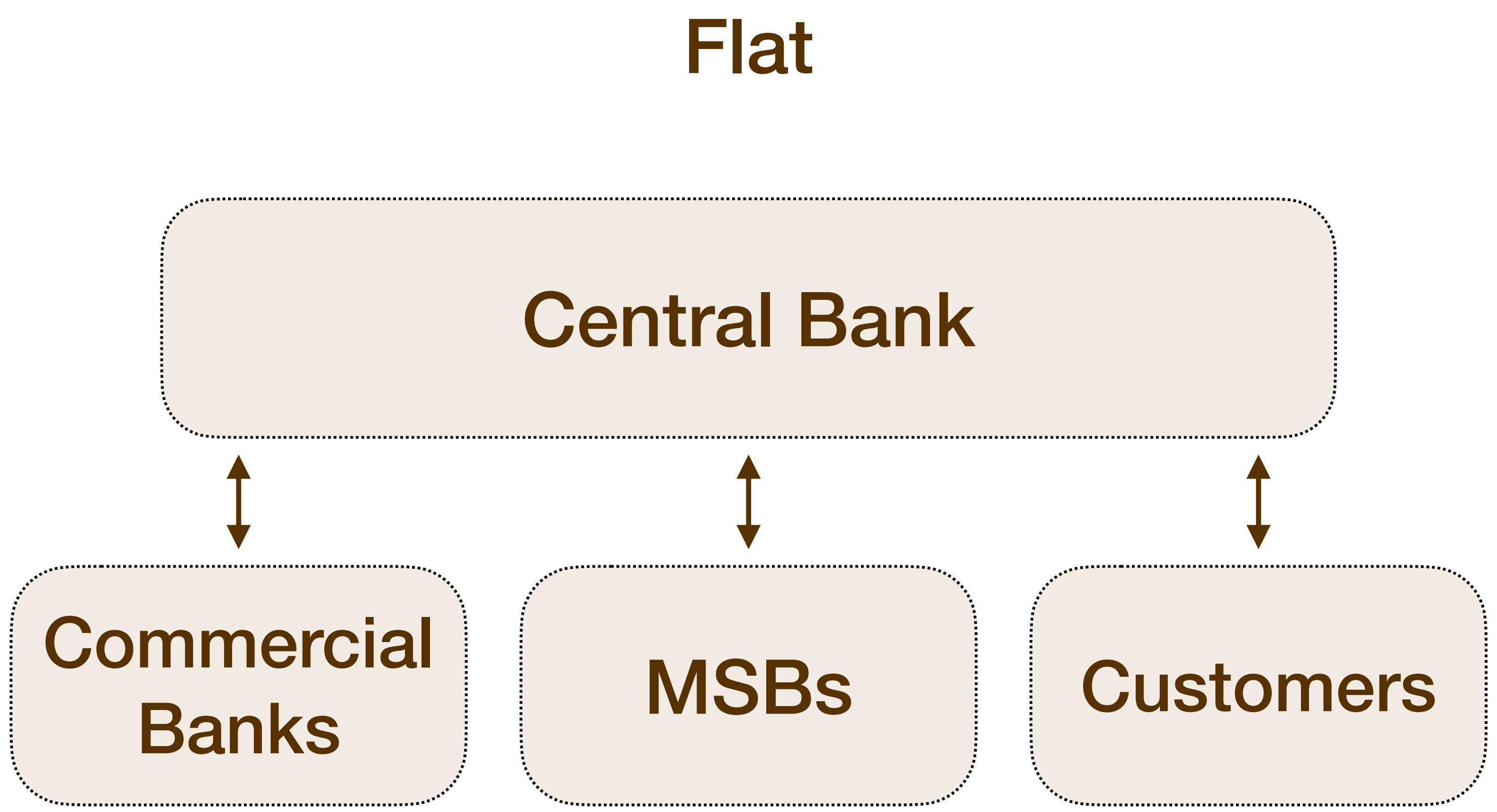
# Distribution

Legacy/Expansive

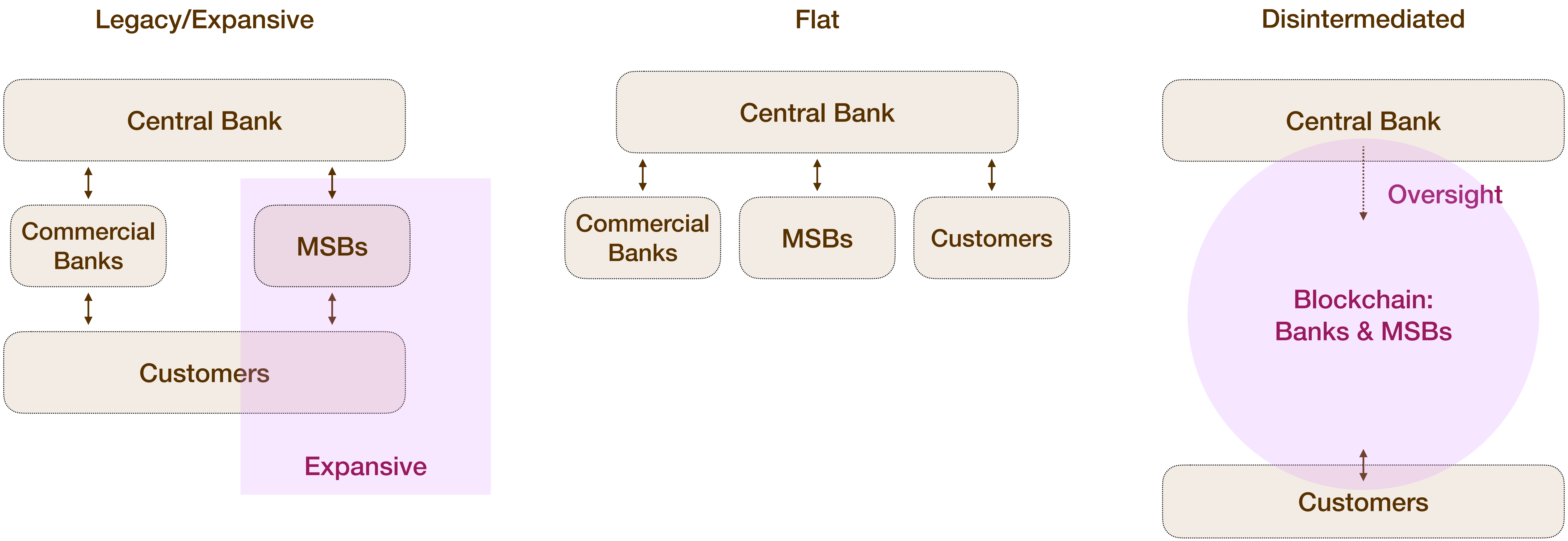


# Distribution



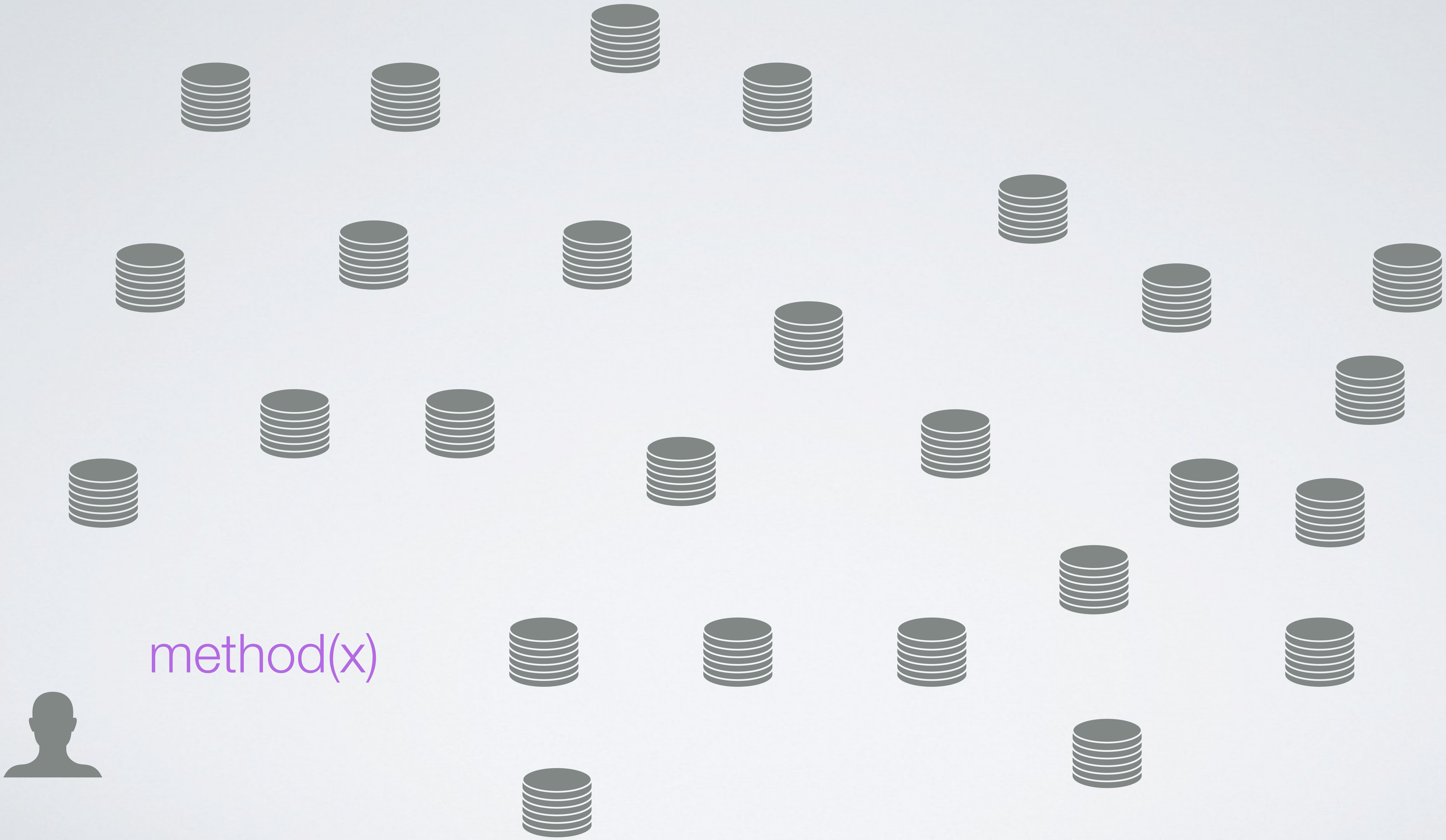


# Distribution

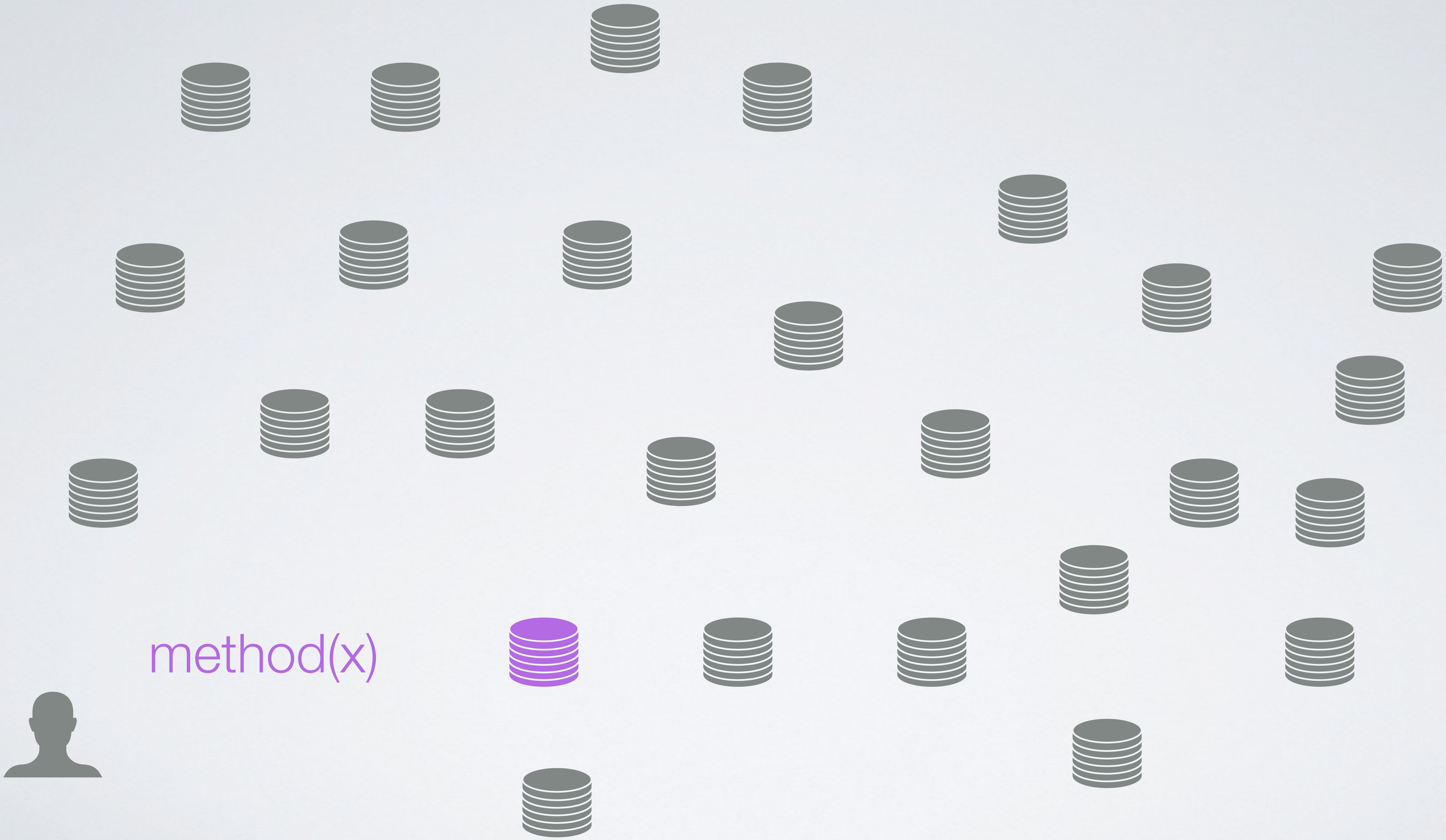


# System Centralization

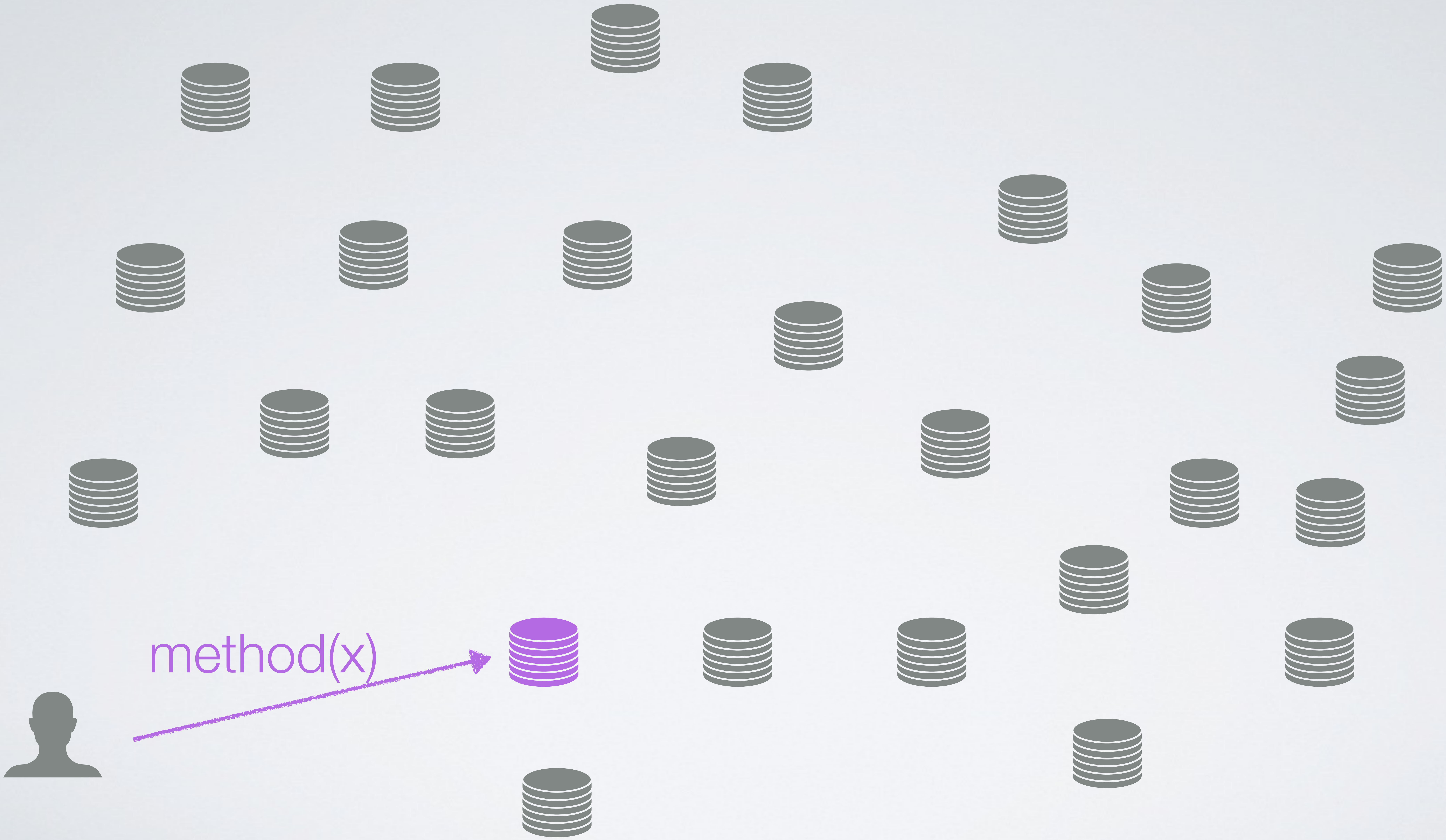
- Blockchain or not?

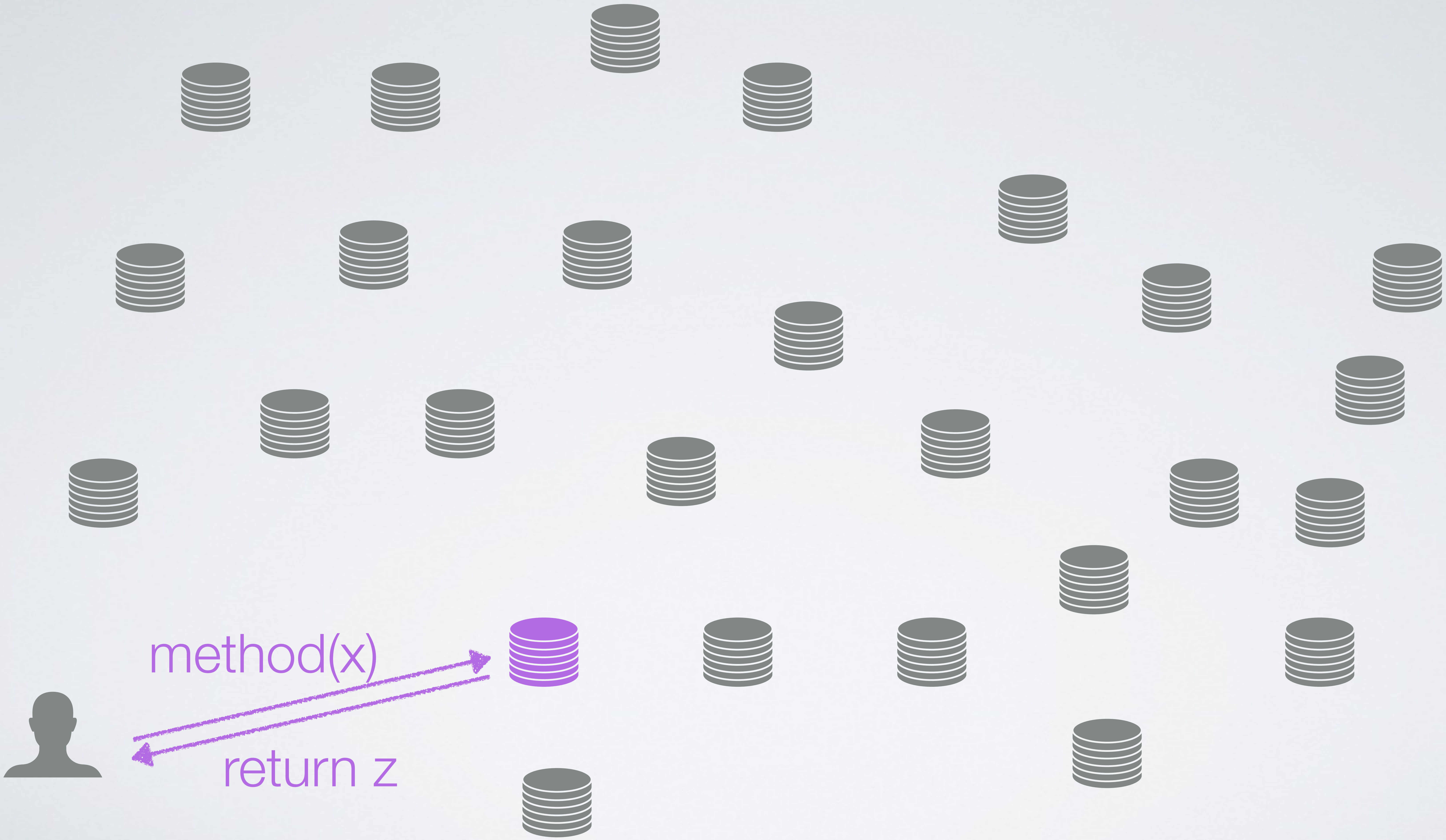


method(x)

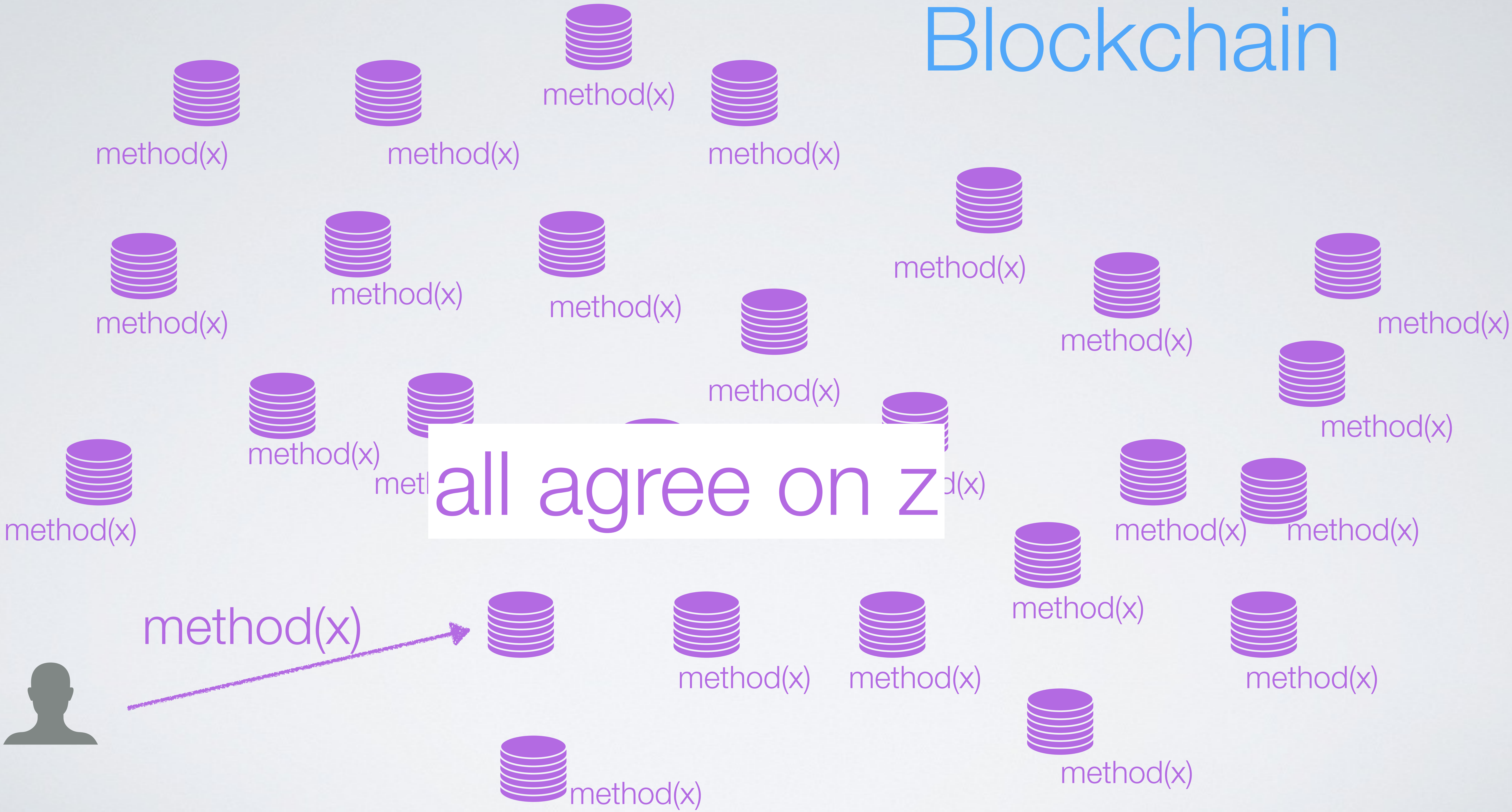


method(x)


method(x)

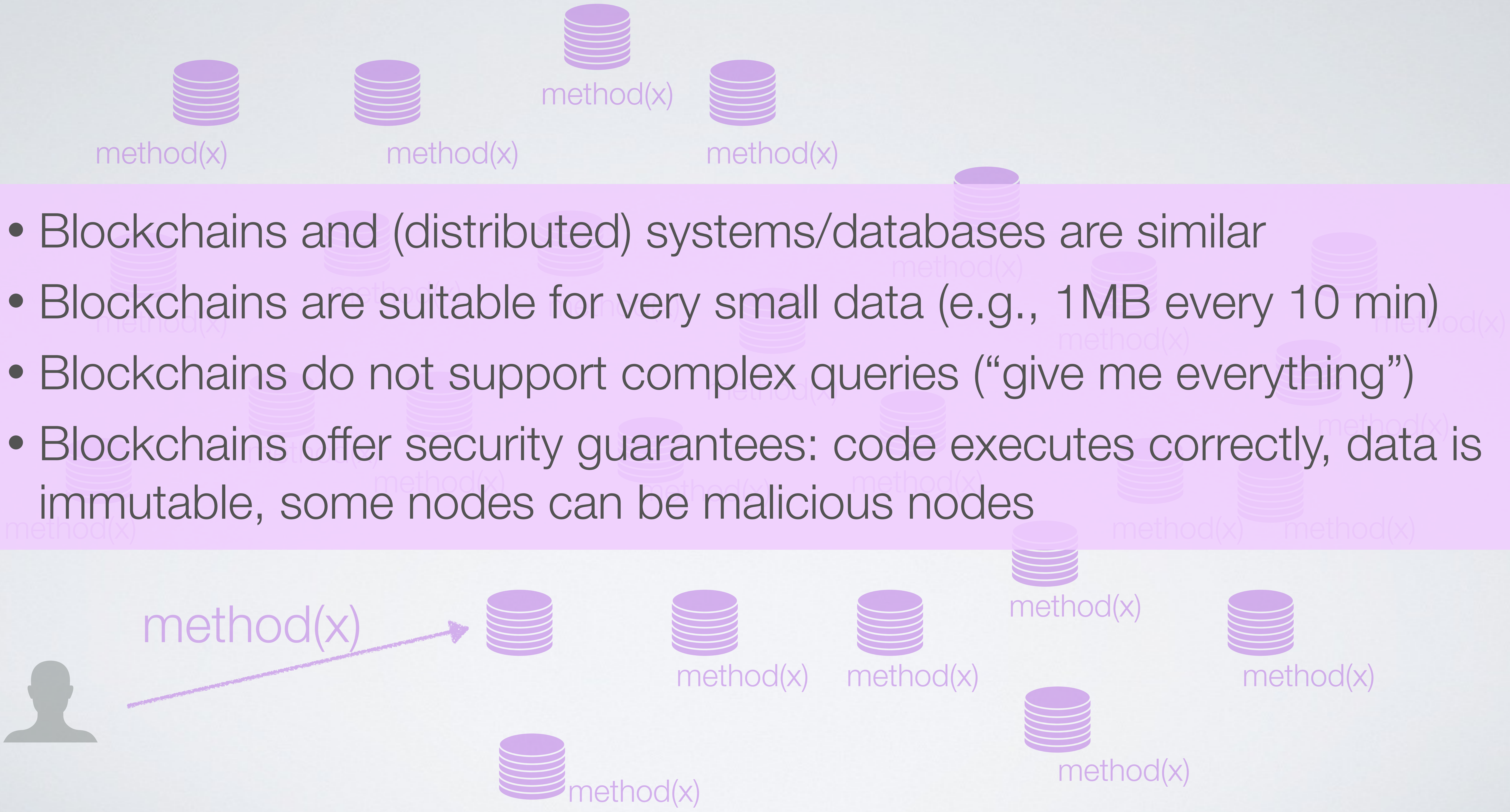

method(x)
return z

# Blockchain



all agree on z

- Blockchains and (distributed) systems/databases are similar
- Blockchains are suitable for very small data (e.g., 1MB every 10 min)
- Blockchains do not support complex queries (“give me everything”)
- Blockchains offer security guarantees: code executes correctly, data is immutable, some nodes can be malicious nodes

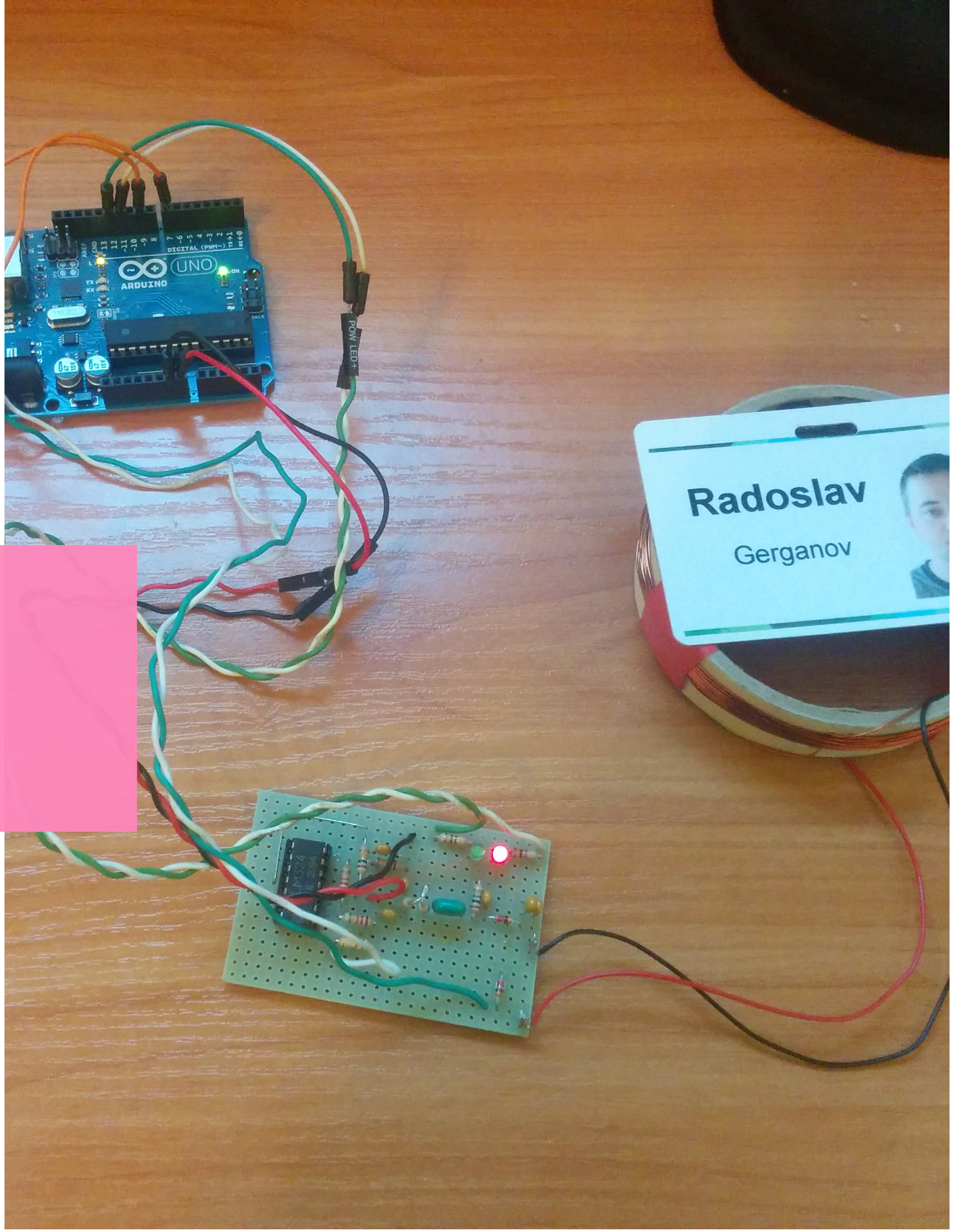


## System Centralization

- Blockchain or not?

## System Functionality

- Payments only
- Payments + Web3

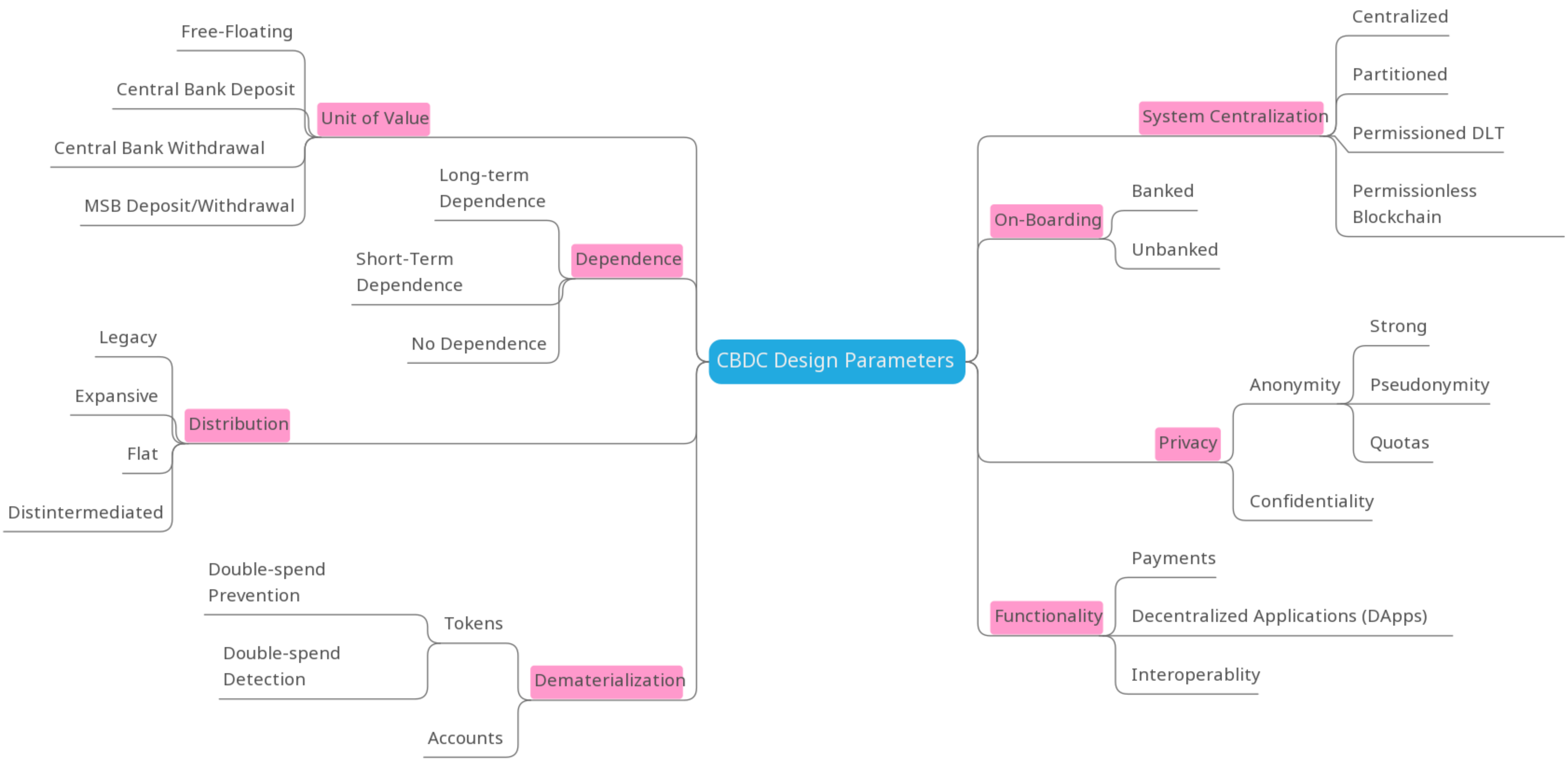


## Dematerialization

- Tokens
- Accounts

Discussion Points:

- Institutional Risks
- Unconventional Monetary Policies (QE, NIRP, Helicopter money)
- Future of Banknotes
- Sanctions
- Data Tracking
- Usability



- CBDC Design Parameters
  - Unit of Value
    - Free-Floating
    - Central Bank Deposit
    - Central Bank Withdrawal
    - MSB Deposit/Withdrawal
  - Dependence
    - Long-term Dependence
    - Short-Term Dependence
    - No Dependence
  - Distribution
    - Legacy
    - Expansive
    - Flat
    - Distintermediated
  - Dematerialization
    - Tokens
      - Double-spend Prevention
      - Double-spend Detection
    - Accounts
  - System Centralization
    - Centralized
    - Partitioned
    - Permissioned DLT
    - Permissionless Blockchain
  - On-Boarding
    - Banked
    - Unbanked
  - Privacy
    - Anonymity
      - Strong
      - Pseudonymity
      - Quotas
    - Confidentiality
  - Functionality
    - Payments
    - Decentralized Applications (DApps)
    - Interoperablity

- CBDC Design Parameters
  - Unit of Value
    - Free-Floating
    - Central Bank Deposit
    - Central Bank Withdrawal
    - MSB Deposit/Withdrawal
  - Dependence
    - Long-term Dependence
    - Short-Term Dependence
    - No Dependence
  - Distribution
    - Legacy
    - Expansive
    - Flat
    - Distintermediated
  - Dematerialization
    - Tokens
      - Double-spend Prevention
      - Double-spend Detection
    - Accounts
  - System Centralization
    - Centralized
    - Partitioned
    - Permissioned DLT
    - Permissionless Blockchain
  - On-Boarding
    - Banked
    - Unbanked
  - Privacy
    - Anonymity
      - Strong
      - Pseudonymity
      - Quotas
    - Confidentiality
  - ments
  - Functionality
    - Decentralized Applications (DApps)
    - Interoperablity

In designing money, national authorities already face a trade-off between satisfying legitimate user preferences for privacy and mitigating risks to financial integrity.

The appropriate degree of privacy, as also judged by society, is a challenge in a digital environment. For CBDC, the appropriate degree of privacy of the currency would need to be considered carefully, which could entail difficult public policy design choices for a central bank.

BIS

**Privacy: The digital dollar will support a balance between individual privacy rights and necessary compliance and regulatory processes, decided upon by policymakers and ultimately reflecting the jurisprudence around the Fourth Amendment**

THE
DIGITAL DOLLAR
PROJECT

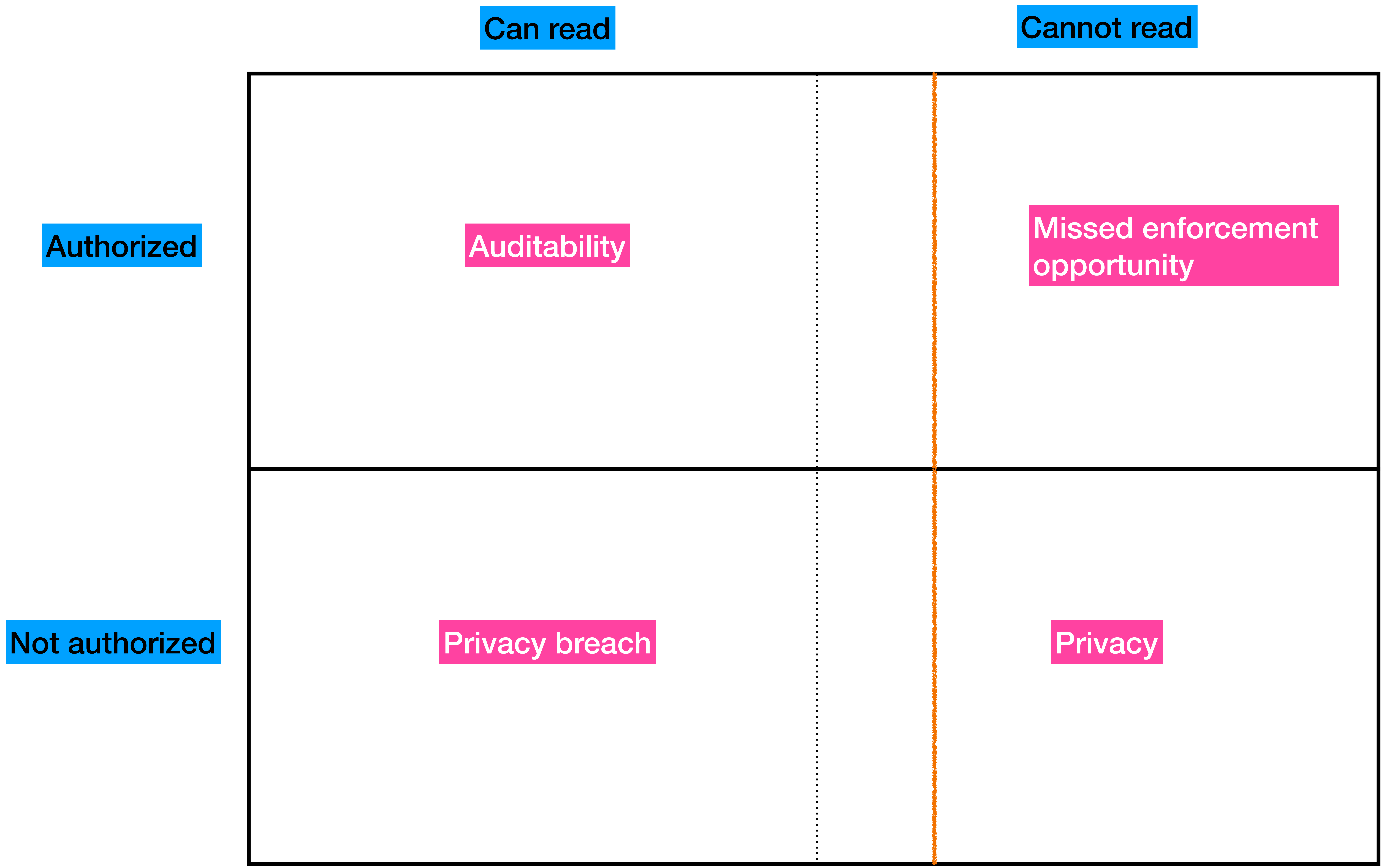
Canadians are concerned about maintaining an appropriate degree of privacy both in relation to private businesses, such as merchants and payment providers, and in relation to the government... How much privacy should be available, and from whom, is an important public policy issue.

BANK OF CANADA
BANQUE DU CANADA

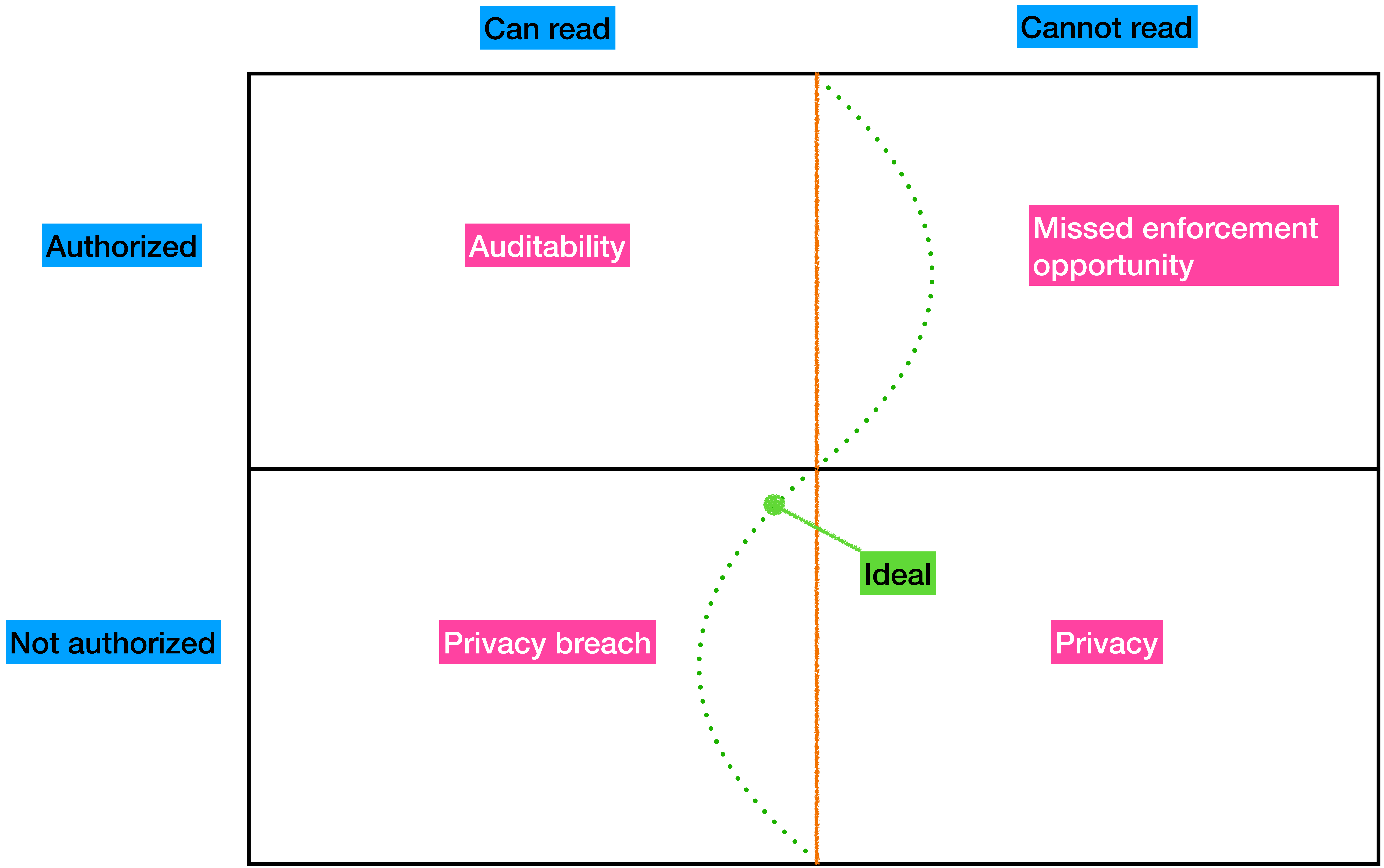
|  | Can read | Cannot read |
|---|---|---|
| Authorized | Auditability |  |
| Not authorized |  | Privacy |

|  | Can read | Cannot read |
|---|---|---|
| Authorized | Auditability | Missed enforcement opportunity |
| Not authorized | Privacy breach | Privacy |

|  | Can read | Cannot read |
|---|---|---|
| Authorized | Auditability | Missed enforcement opportunity |
| Not authorized | Privacy breach | Privacy |



| | Can read | Cannot read |
|---|---|---|
| Authorized | Auditability | Missed enforcement opportunity |
| Not authorized | Privacy breach | Privacy |



| | Can read | Cannot read |
|---|---|---|
| Authorized | Auditability | Missed enforcement opportunity |
| Not authorized | Privacy breach | Privacy |

Many Stakeholders

- Central Banks
- Established Commercial Banks
- Emergent Commercial Banks
- Payment Providers
- Enforcement: AML
- Enforcement: ATF (CFT)
- Enforcement: Financial Crimes
- Enforcement: Tax Avoidance
- Depository Insurance
- Federal Government
- Typical Residents/Citizens
- Vulnerable Residents/Citizens
- Unbanked
- Foreign nationals
- Tourists
- Investigative Journalists

Key Stakeholders:

- Law enforcement: Prevent crime that involves payments
- Data holders: Commercial banks, payment processors and merchants
- Privacy enthusiasts: Typical users, regulators, privacy advocates

- **Key conflicts:**

**Law enforcement**

**Data holders**

**Privacy enthusiasts**

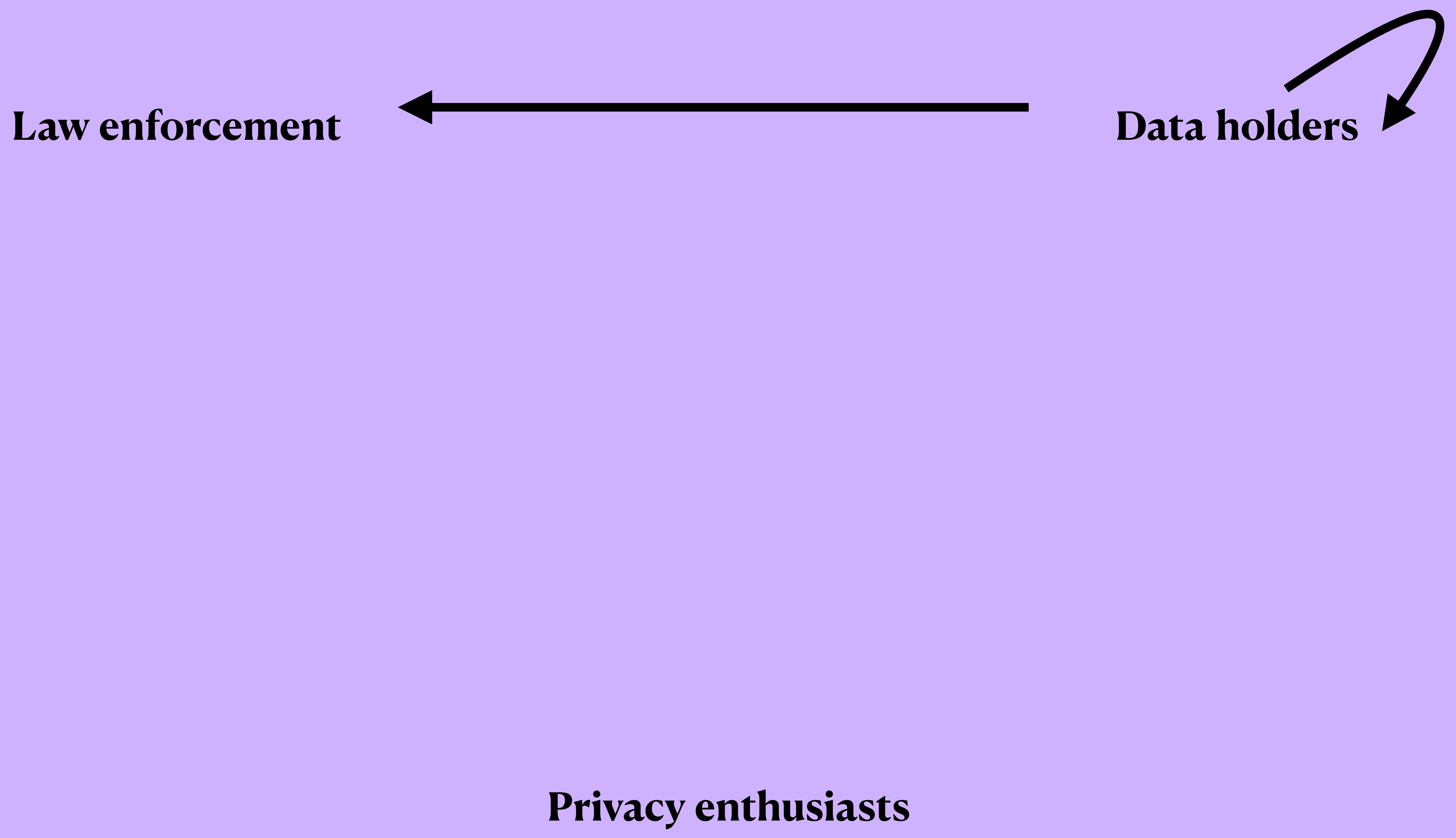
- Key conflicts:
  - Law enforcement want to ensure someone can service their authorized requests for financial data, but are neutral on who

Law enforcement

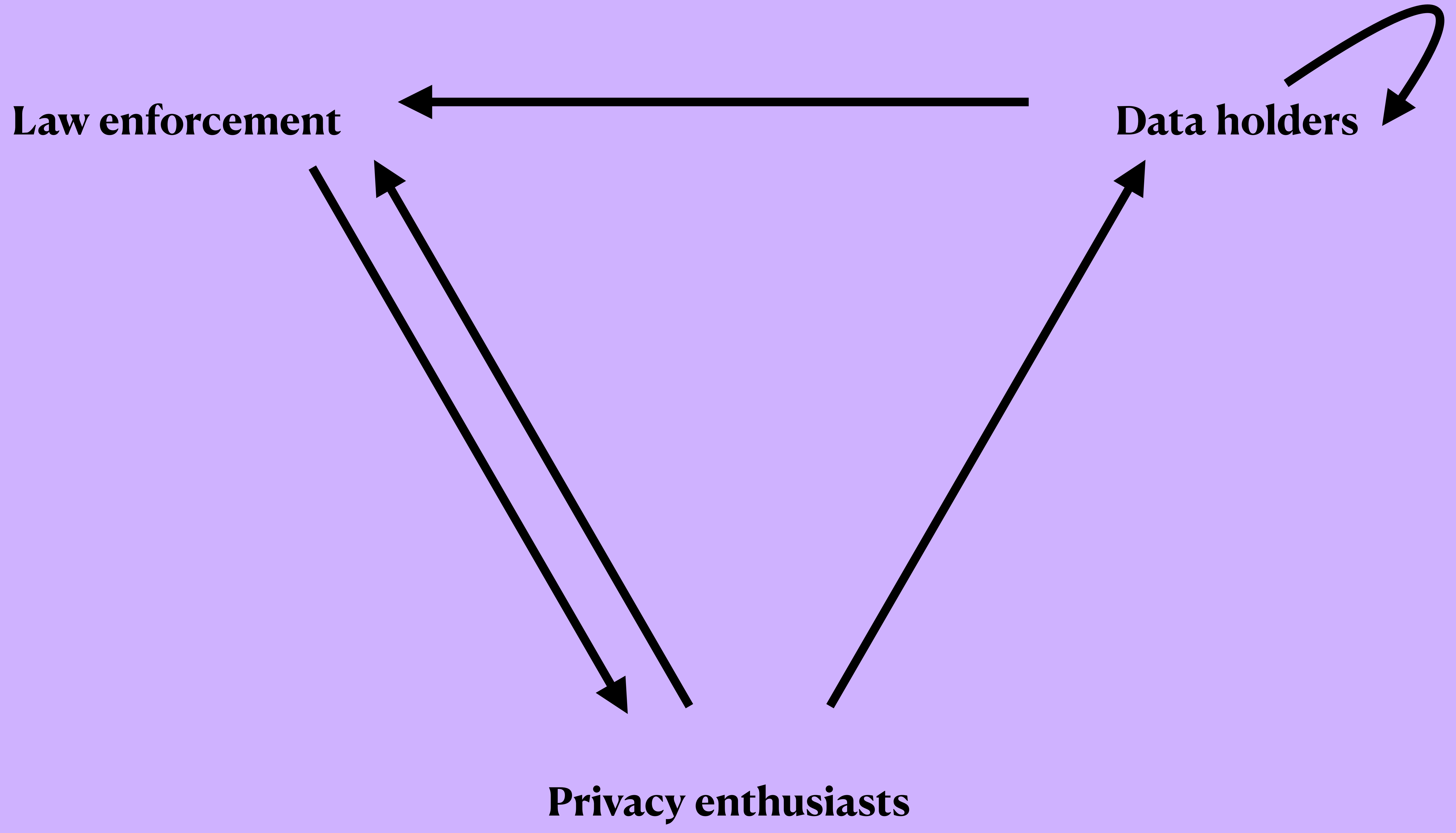
Data holders

Privacy enthusiasts

- Key conflicts:
  - Data holders wish to avoid the expense of servicing law enforcement and regulations
  - Data holders have internal conflicts over the exclusivity of their financial data, which can be monetized



- Key conflicts:
  - Privacy enthusiasts oppose indirect collection and monetization of their personal information
  - Privacy enthusiasts support low crime rates but are concerned about law enforcement mistakes, corruptions and overreach
  - Law enforcement is concerned with the impediments to investigations posed by privacy enhancing technologies



| | Law enforcement | Privacy enthusiasts | | Data holders | |
|---|---|---|---|---|---|
| | L → P | P → D | P → L | D → D | D → L |
| Cash | Ok | | | | |
| Payment Network | Good | | | | |
| Cryptocurrency | Ok/Bad | | | | |
| Soft Privacy CBDC | Good | | | | |
| Hard Privacy CBDC | Ok | | | | |

| | Law enforcement | Privacy enthusiasts | | Data holders | |
|---|---|---|---|---|---|
| | L → P | P → D | P → L | D → D | D → L |
| Cash | Ok | Good | | | |
| Payment Network | Good | Bad | | | |
| Cryptocurrency | Ok/Bad | Good | | | |
| Soft Privacy CBDC | Good | Bad | | | |
| Hard Privacy CBDC | Ok | Ok | | | |

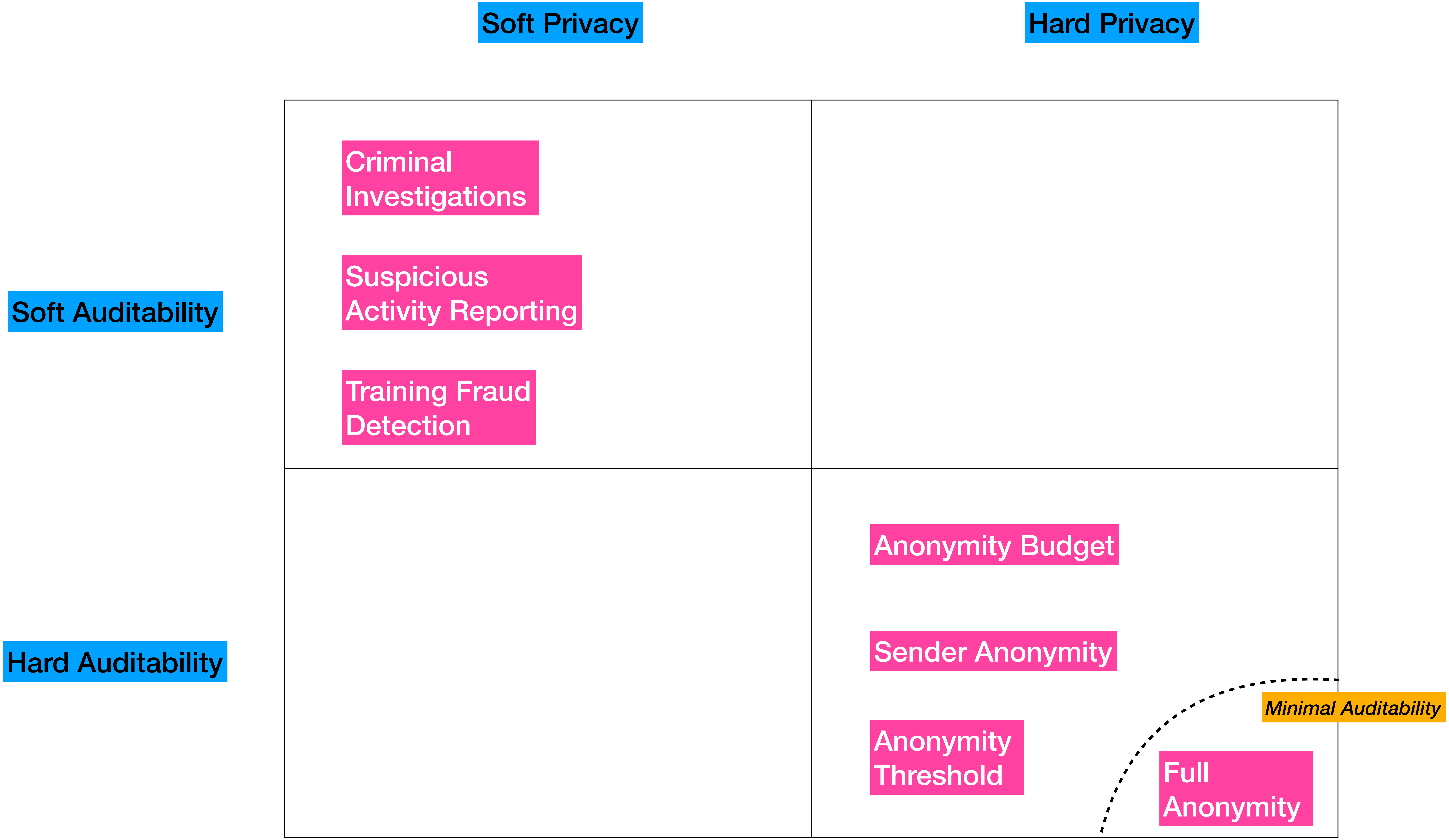
|  | Law enforcement | Privacy enthusiasts |  | Data holders |  |
|---|---|---|---|---|---|
|  | L → P | P → D | P → L | D → D | D → L |
| **Cash** | Ok | Good | Good |  |  |
| **Payment Network** | Good | Bad | Bad |  |  |
| **Cryptocurrency** | Ok/Bad | Good | Good |  |  |
| **Soft Privacy CBDC** | Good | Bad | Ok |  |  |
| **Hard Privacy CBDC** | Ok | Ok | Good |  |  |

|  | Law enforcement | Privacy enthusiasts |  | Data holders |  |
|---|---|---|---|---|---|
|  | L → P | P → D | P → L | D → D | D → L |
| **Cash** | Ok | Good | Good | Good |  |
| **Payment Network** | Good | Bad | Bad | Neutral |  |
| **Cryptocurrency** | Ok/Bad | Good | Good | Good |  |
| **Soft Privacy CBDC** | Good | Bad | Ok | Good/Bad |  |
| **Hard Privacy CBDC** | Ok | Ok | Good | Good/Bad |  |

| | Law enforcement | Privacy enthusiasts | | Data holders | |
|---|---|---|---|---|---|
| | L → P | P → D | P → L | D → D | D → L |
| Cash | Ok | Good | Good | Good | Neutral |
| Payment Network | Good | Bad | Bad | Neutral | Neutral |
| Cryptocurrency | Ok/Bad | Good | Good | Good | Neutral |
| Soft Privacy CBDC | Good | Bad | Ok | Good/Bad | Neutral |
| Hard Privacy CBDC | Ok | Ok | Good | Good/Bad | Bad |

|  | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability |  |  |
| Hard Auditability |  |  |

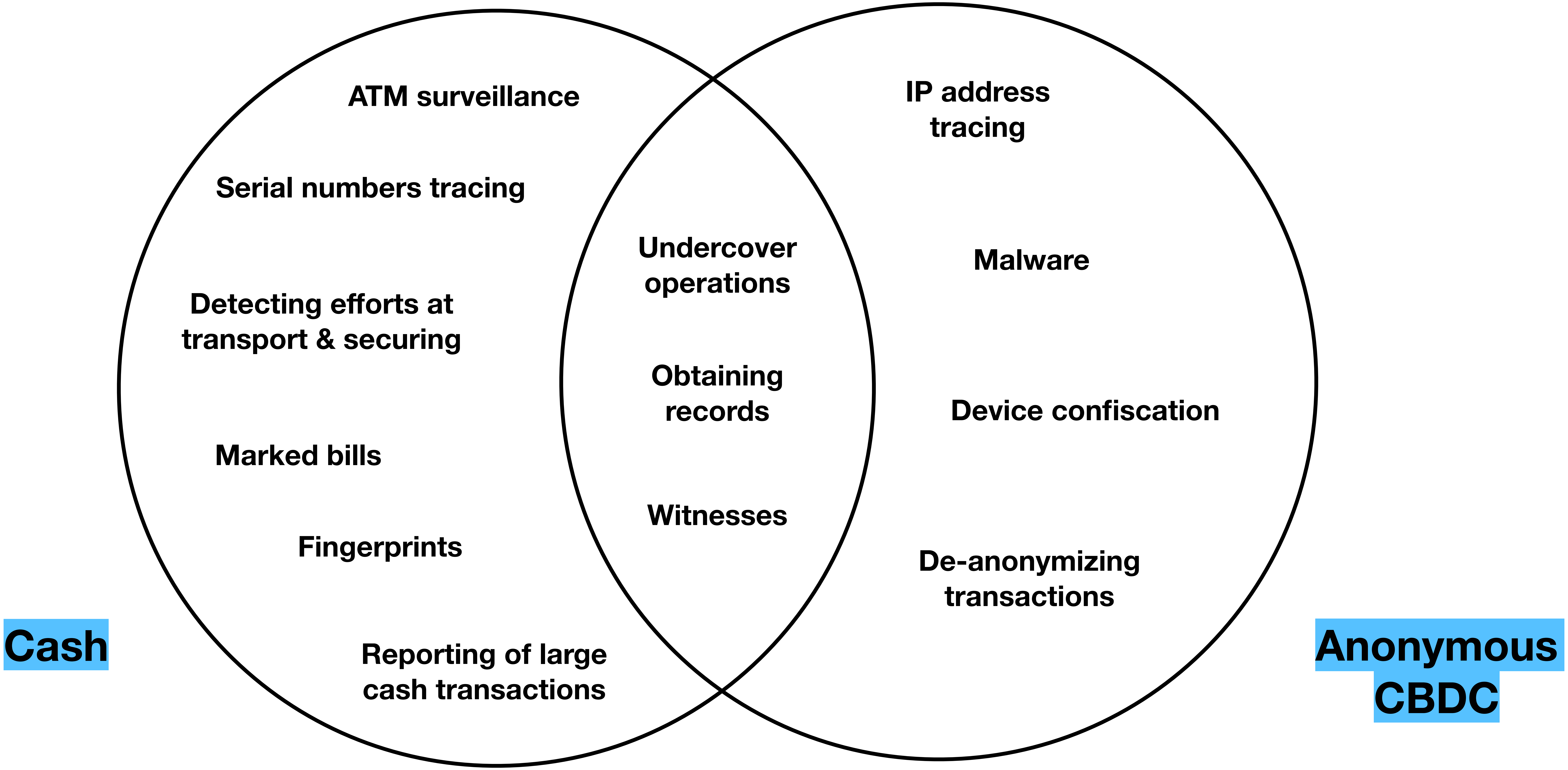
| | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability | Criminal Investigations<br>Suspicious Activity Reporting<br>Training Fraud Detection | |
| Hard Auditability | | |



|  | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability | Criminal Investigations<br>Suspicious Activity Reporting<br>Training Fraud Detection |  |
| Hard Auditability |  | Anonymity Budget<br>Sender Anonymity<br>Anonymity Threshold<br>Full Anonymity |

*Minimal Auditability*

# Possible Investigative Techniques



Cash

ATM surveillance

Serial numbers tracing

Detecting efforts at transport & securing

Marked bills

Fingerprints

Reporting of large cash transactions

Undercover operations

Obtaining records

Witnesses

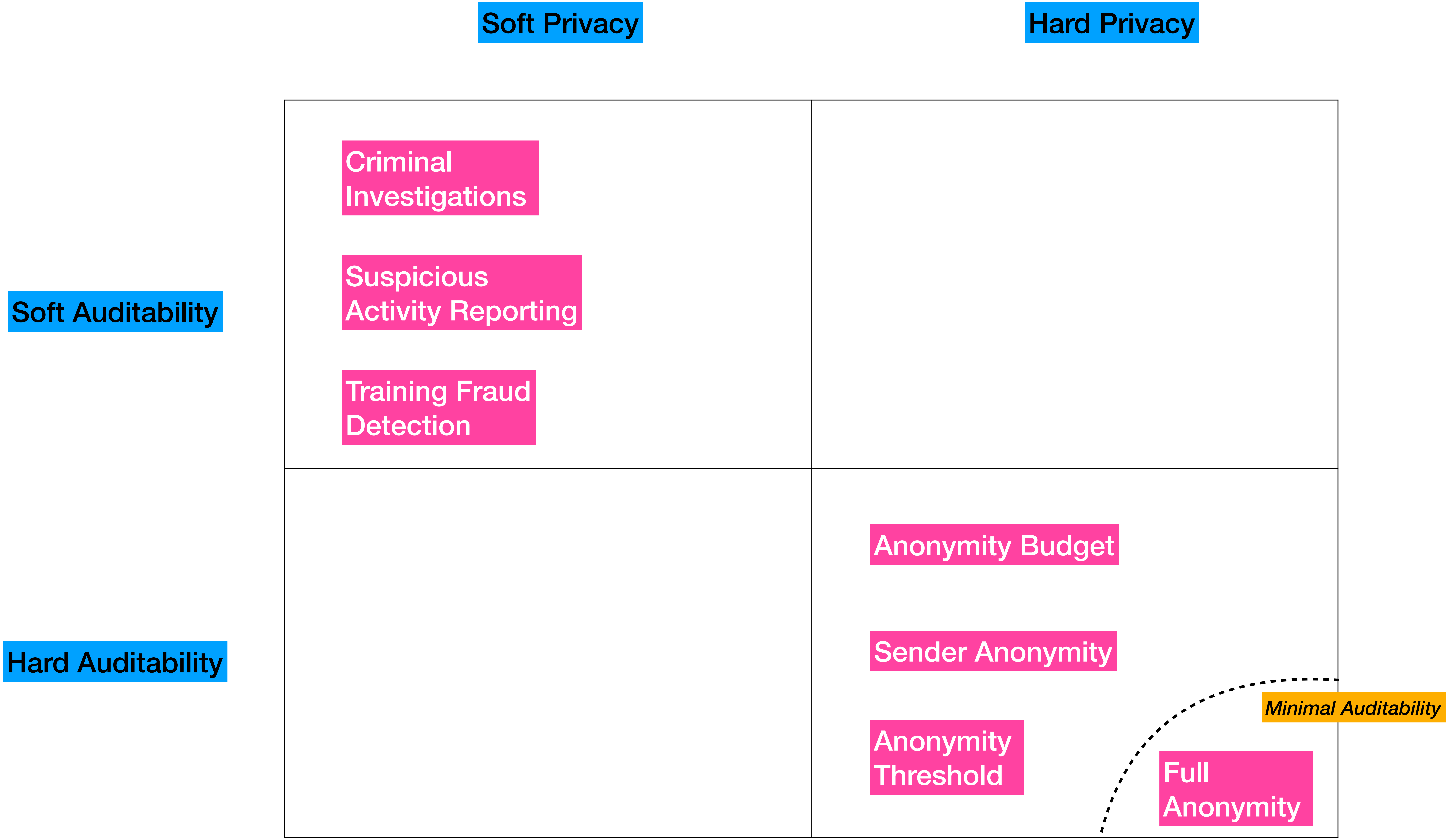
Anonymous CBDC

IP address tracing

Malware

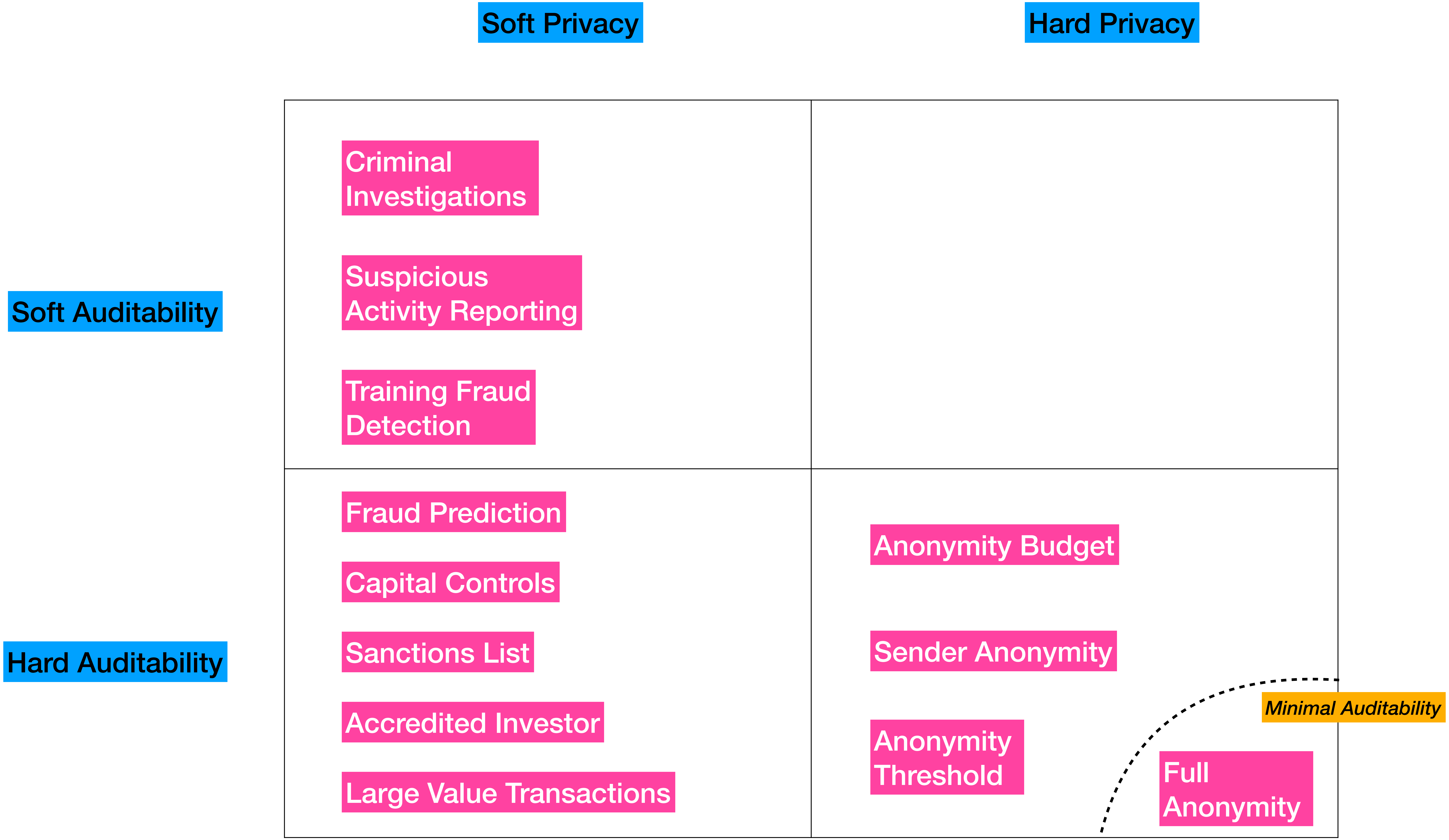
Device confiscation

De-anonymizing transactions

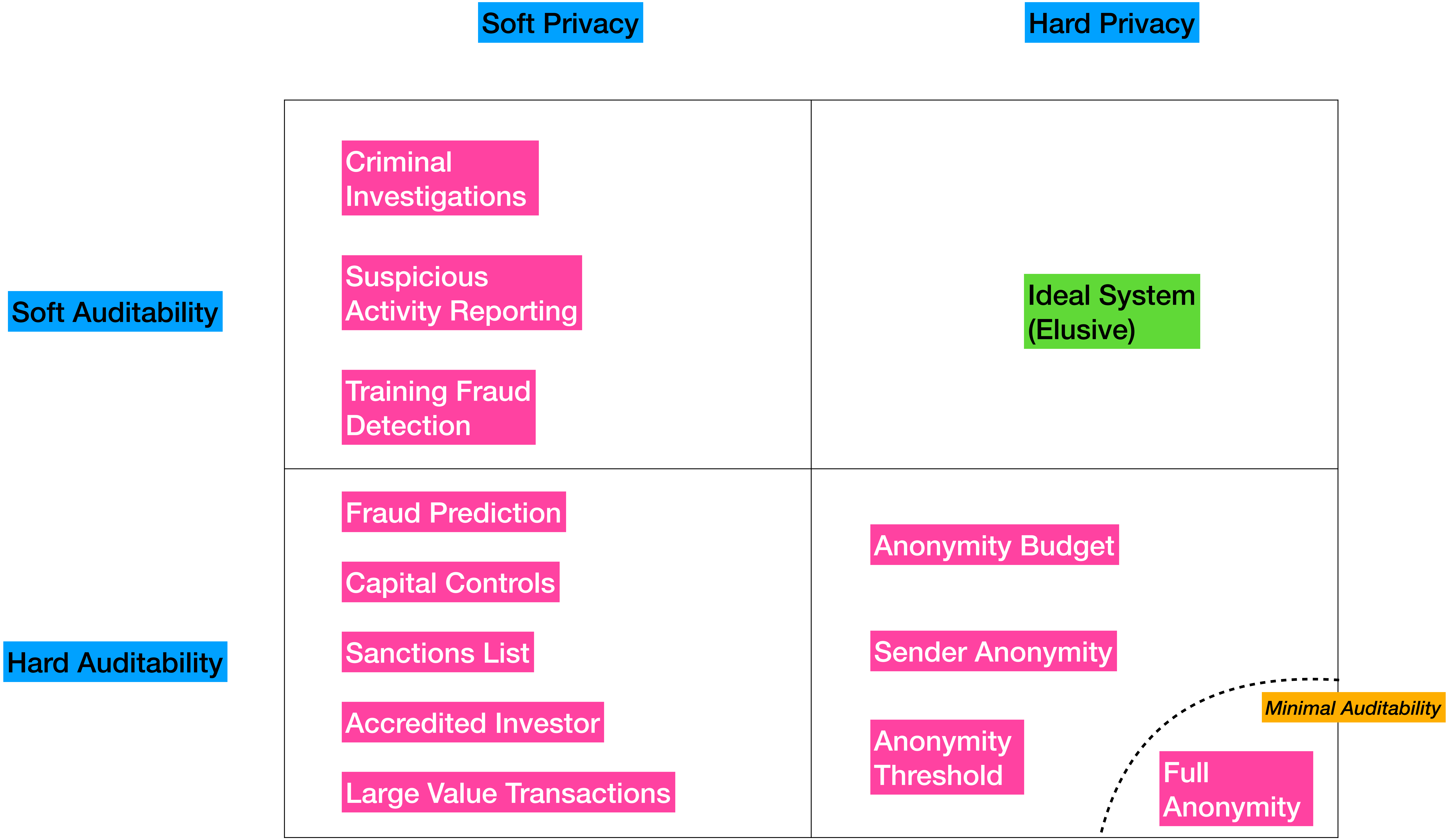


| | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability | Criminal Investigations<br>Suspicious Activity Reporting<br>Training Fraud Detection | |
| Hard Auditability | | Anonymity Budget<br>Sender Anonymity<br>Anonymity Threshold<br>Full Anonymity |

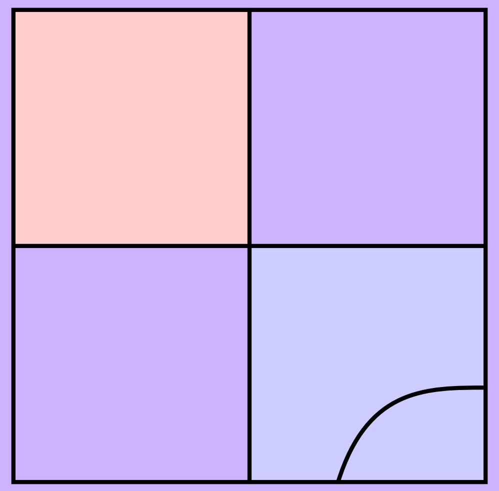
*Minimal Auditability*



| | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability | Criminal Investigations<br>Suspicious Activity Reporting<br>Training Fraud Detection | |
| Hard Auditability | Fraud Prediction<br>Capital Controls<br>Sanctions List<br>Accredited Investor<br>Large Value Transactions | Anonymity Budget<br>Sender Anonymity<br>Anonymity Threshold<br>Full Anonymity |



| | Soft Privacy | Hard Privacy |
|---|---|---|
| Soft Auditability | Criminal Investigations<br>Suspicious Activity Reporting<br>Training Fraud Detection | Ideal System (Elusive) |
| Hard Auditability | Fraud Prediction<br>Capital Controls<br>Sanctions List<br>Accredited Investor<br>Large Value Transactions | Anonymity Budget<br>Sender Anonymity<br>Anonymity Threshold<br>*Minimal Auditability*<br>Full Anonymity |



| *Privacy type* | *Example* | Money laundering | Hiding insolvency | Tax evasion | Asset smuggling | Terrorist financing | Bribery | Embezzlement | Extortion | Robbery | Fugitive hunt |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Soft privacy & soft auditability** | Electronic retail | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| **Hard privacy & hard auditability** | | | | | | | | | | | |
| Full anonymity | zcash | | | | | | | | | | |
| Privacy for payers | GNU Taler | | | ● | | ● | ● | | ● | | |
| Privacy for payees | Stealth address | | | | | | | | | | ● |
| Privacy threshold | PRCash | ● | | | ● | ● | | | ● | | |
| Privacy budget | UTT | ● | | | ● | ● | | ● | ● | | |
| Privacy w/ aggregate disclosure | zkLedger | | ● | ● | | | | ● | | | |
| Privacy with alibi | Monero | ○ | | ○ | ○ | ○ | ○ | | ○ | | |

## THREAT ACTORS

D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS

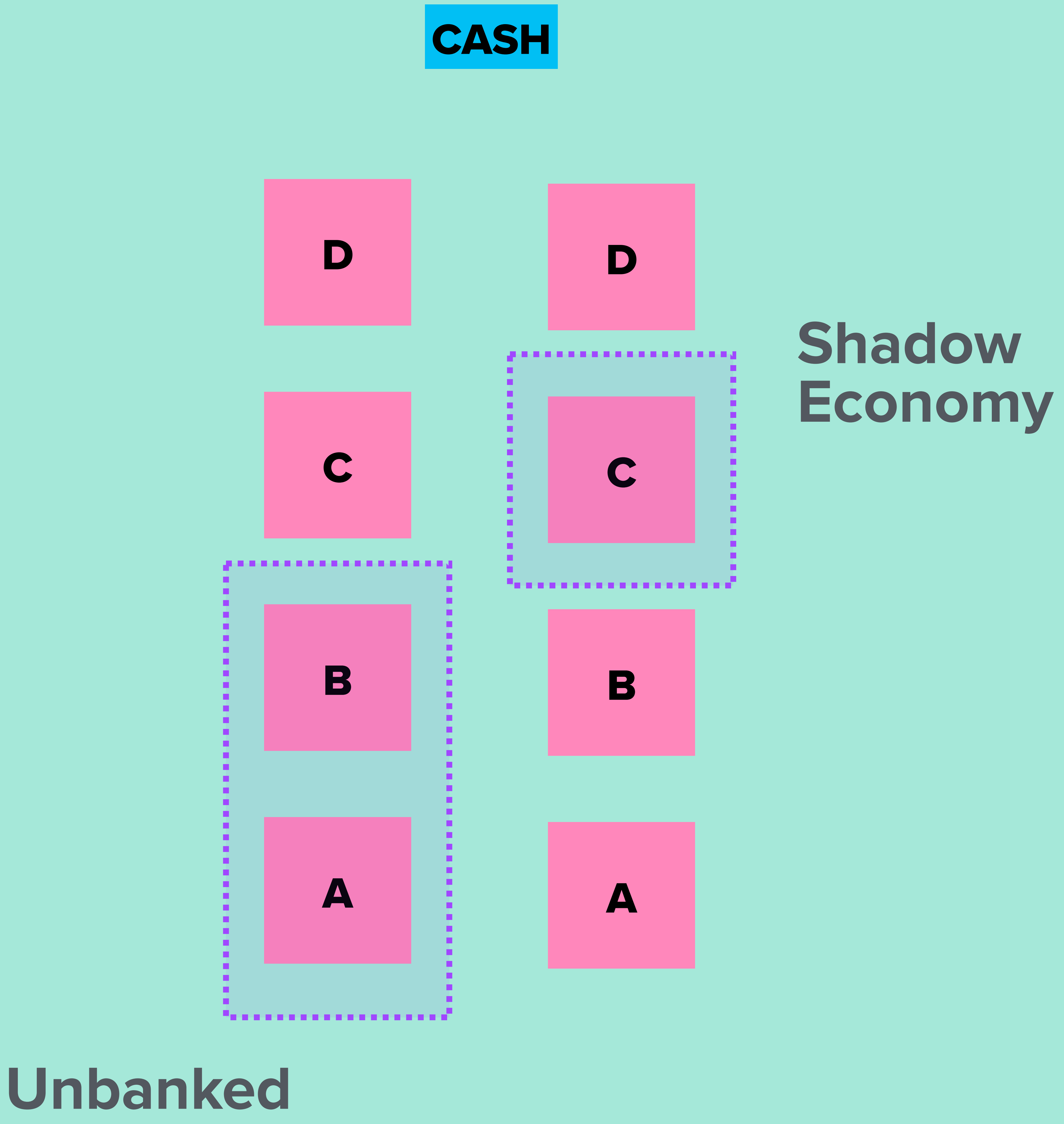
## THREAT ACTORS

D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS



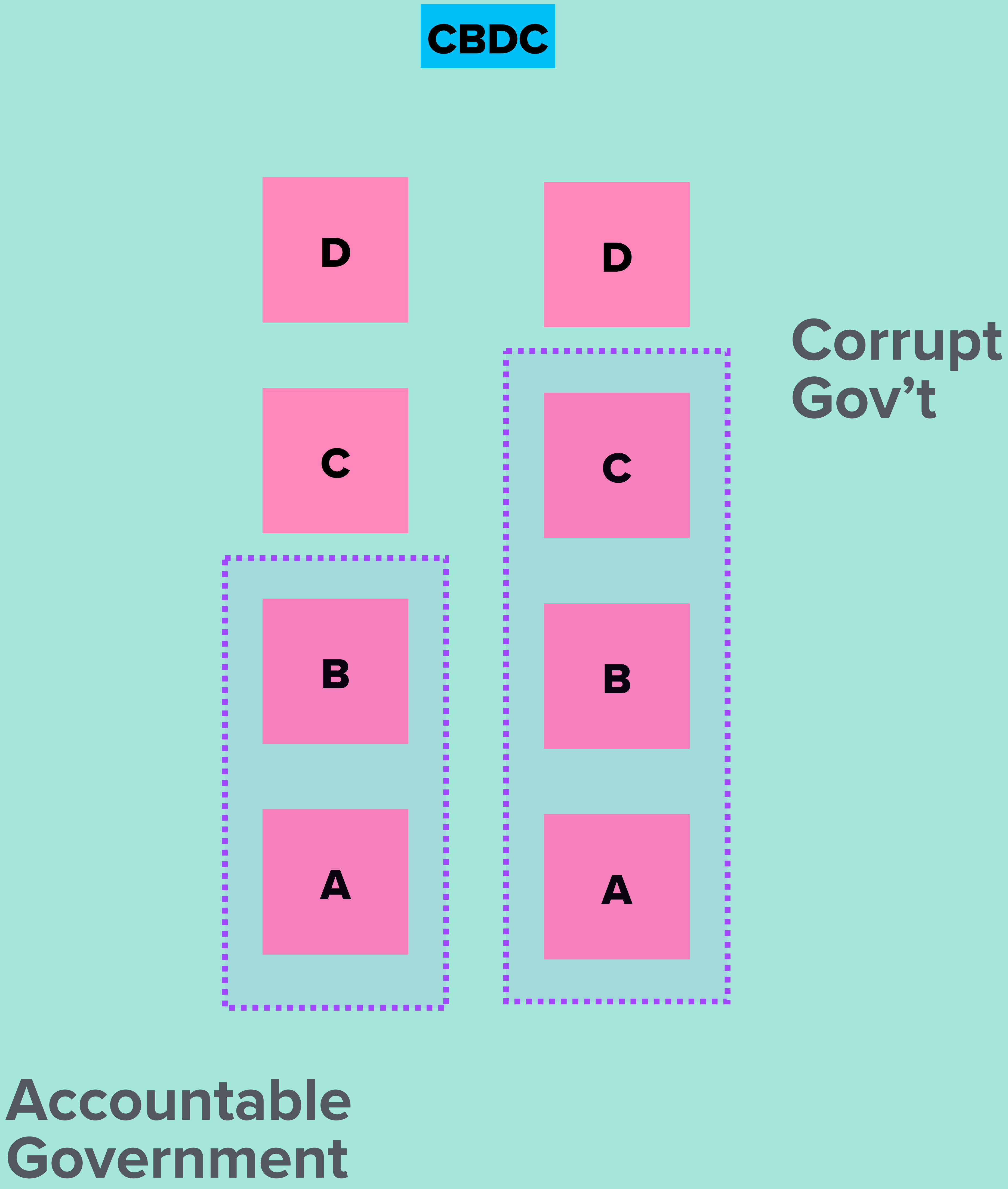
## THREAT ACTORS

D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS



CBDC

D

C

B

A

Accountable Government

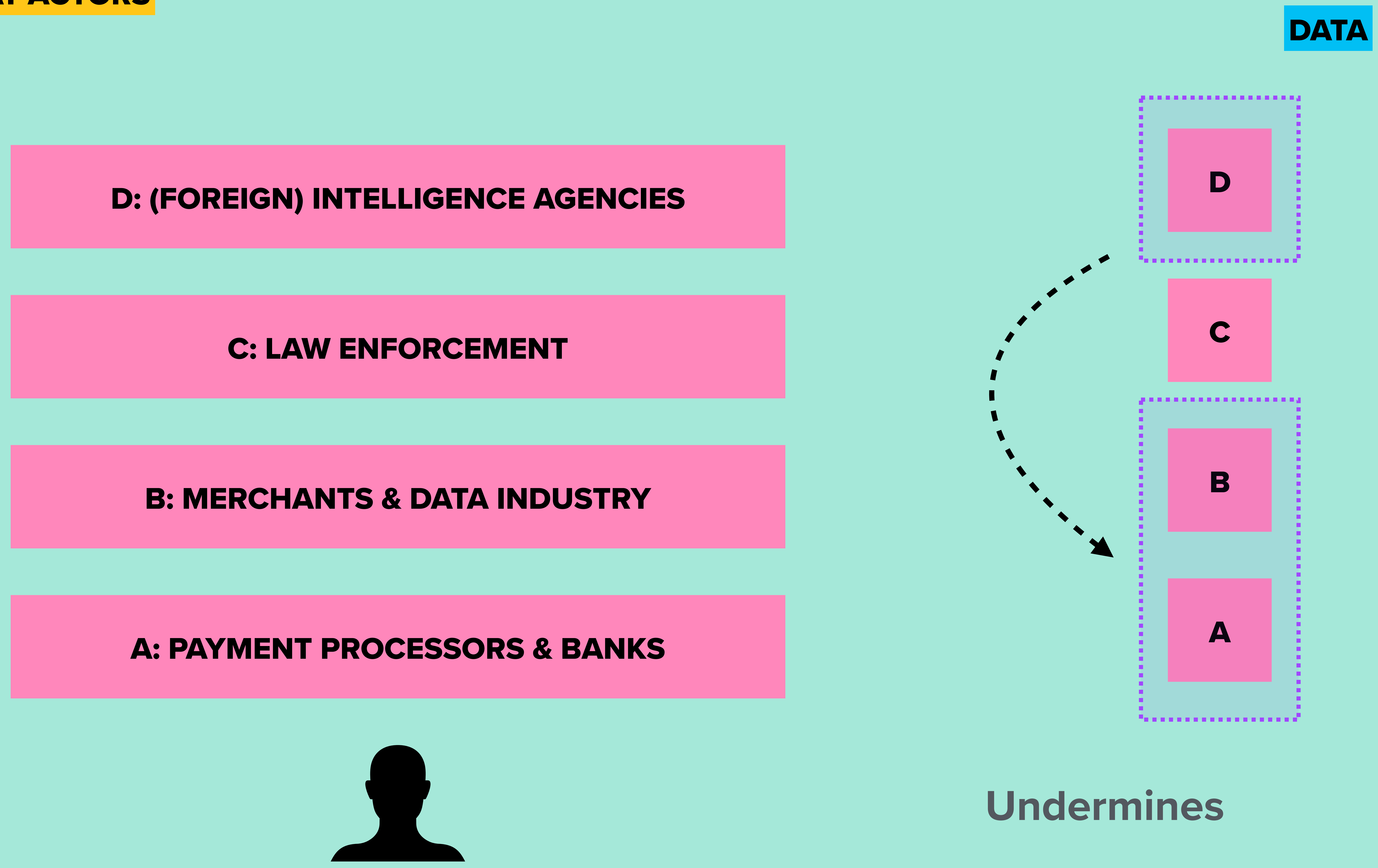
D

C

B

A

Corrupt Gov't



THREAT ACTORS

D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS

Undermines

THREAT ACTORS

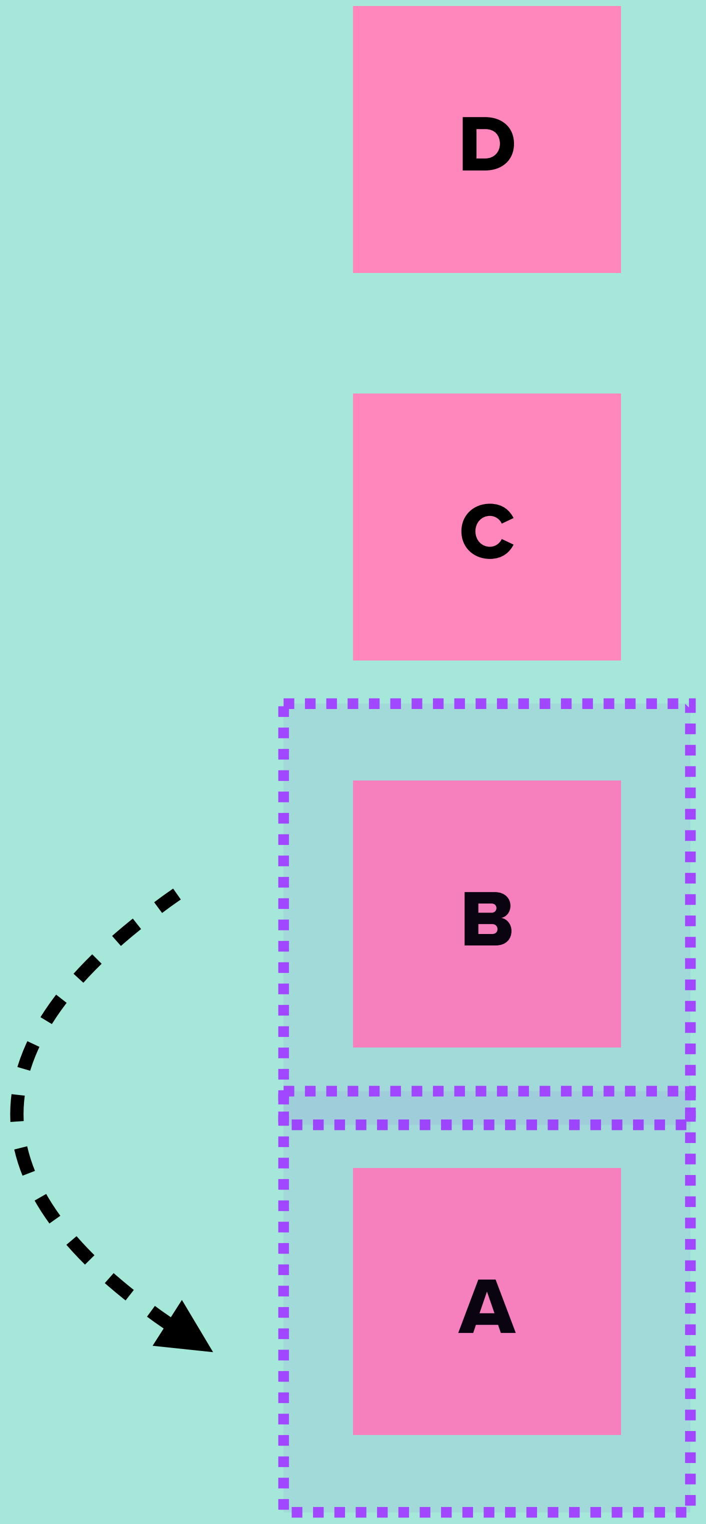
D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS

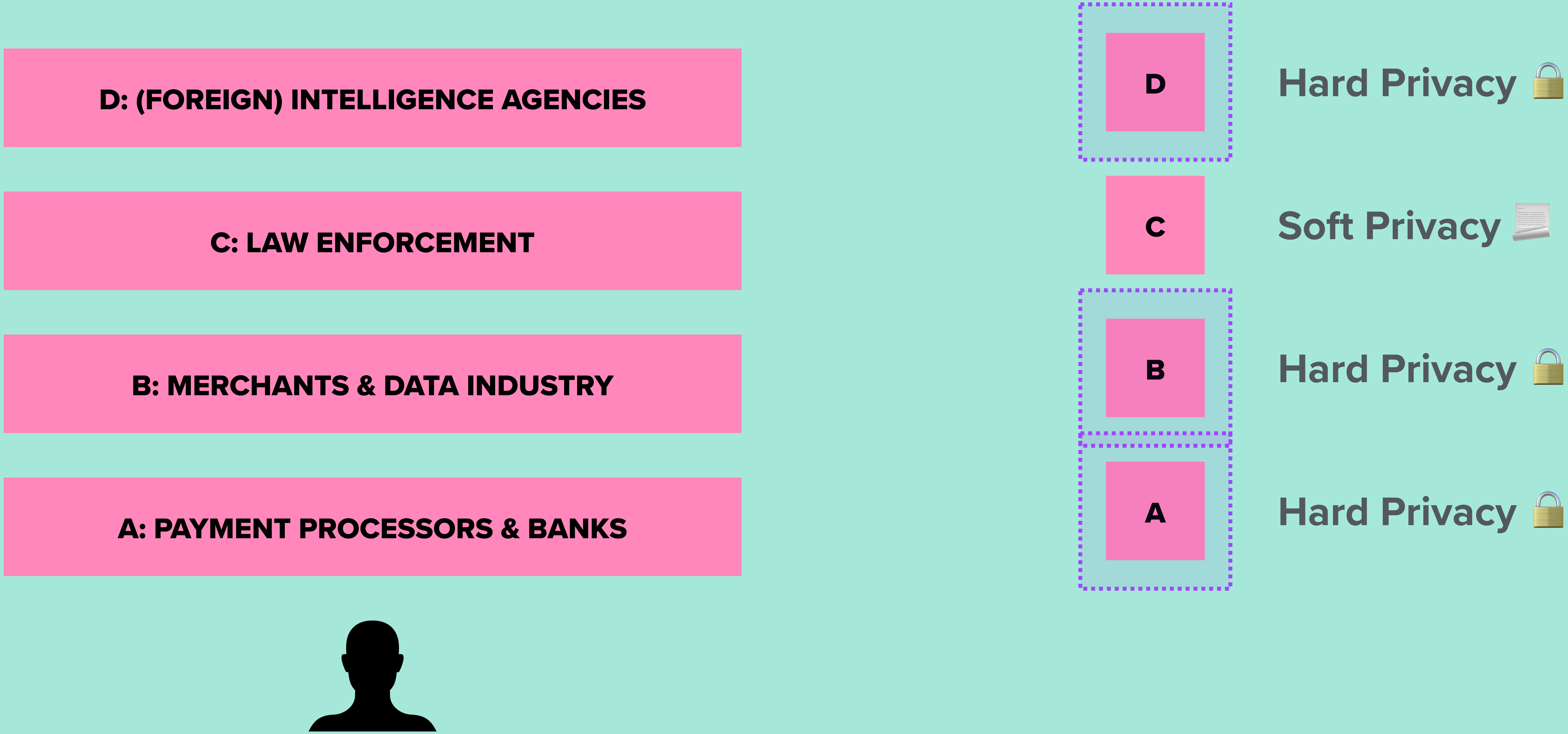
DATA



Undermines

THREAT ACTORS

DATA



D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: PAYMENT PROCESSORS & BANKS

D

C

B

A

Hard Privacy 🔒

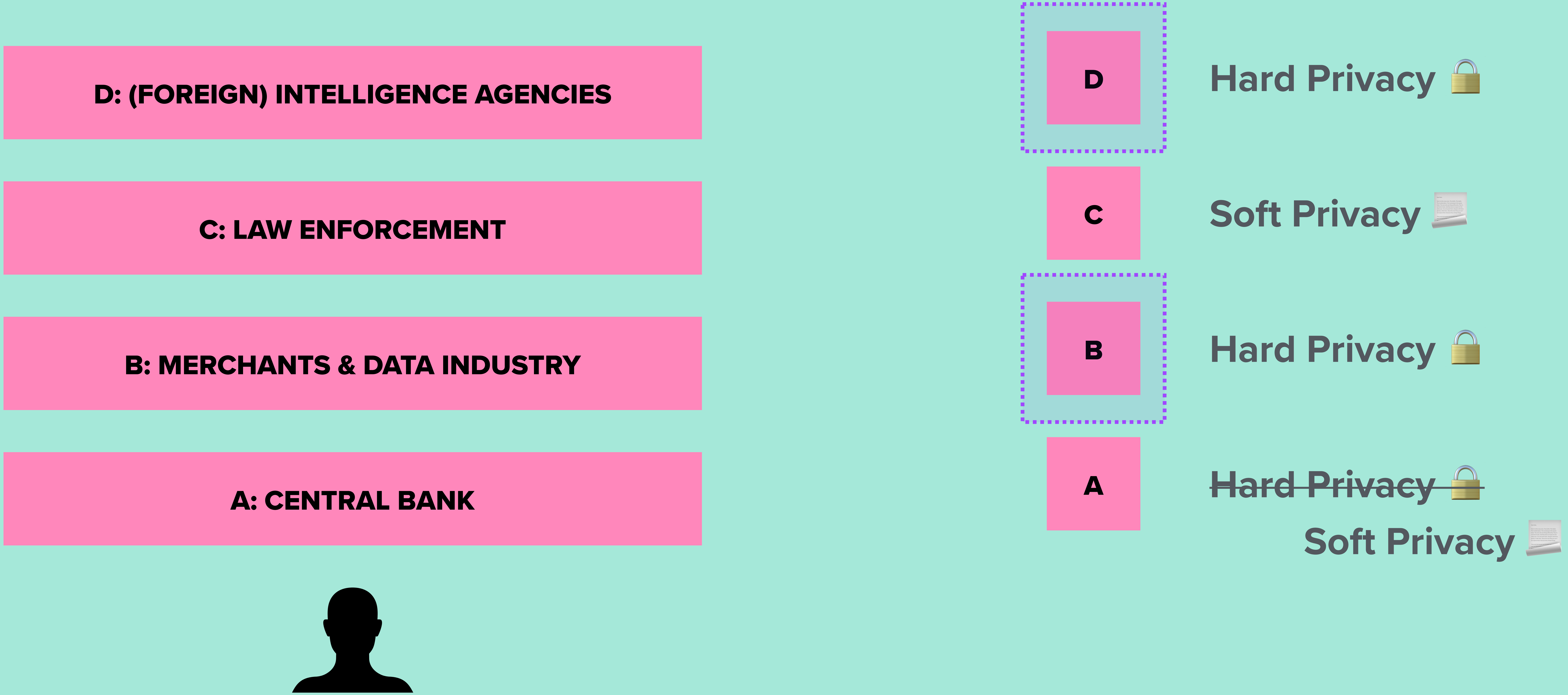
Soft Privacy 📜

Hard Privacy 🔒

Hard Privacy 🔒

THREAT ACTORS

DATA



D: (FOREIGN) INTELLIGENCE AGENCIES

C: LAW ENFORCEMENT

B: MERCHANTS & DATA INDUSTRY

A: CENTRAL BANK

Hard Privacy 🔒

Soft Privacy 📜

Hard Privacy 🔒

~~Hard Privacy 🔒~~

Soft Privacy 📜

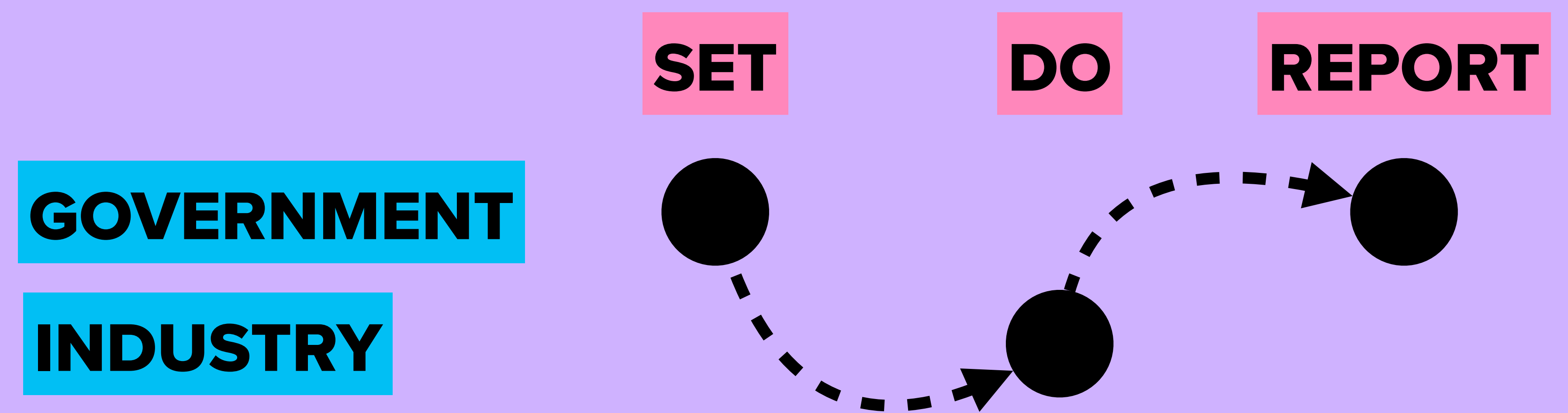
- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
    - Complex logistics
    - On-boarding every user is expensive
    - Disruption to the banking industry

- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
  - Complex logistics
  - On-boarding every user is expensive
  - Disruption to the banking industry

- Arguments from a privacy perspective <u>for</u> a direct CBDC:
  - Central banks are trustworthy on data privacy issues
  - Financial tracking rules are streamlined

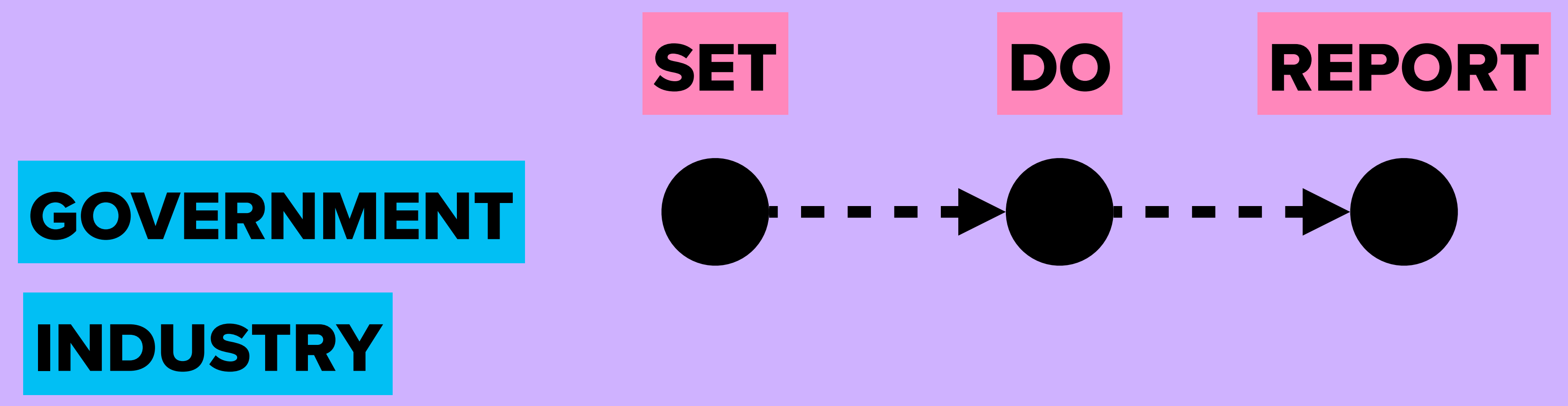
- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
  - Complex logistics
  - On-boarding every user is expensive
  - Disruption to the banking industry

- Arguments from a privacy perspective for a direct CBDC:
  - Central banks are trustworthy on data privacy issues
  - Financial tracking rules are streamlined



- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
  - Complex logistics
  - On-boarding every user is expensive
  - Disruption to the banking industry

- Arguments from a privacy perspective for a direct CBDC:
  - Central banks are trustworthy on data privacy issues
  - Financial tracking rules are streamlined



SET

DO

REPORT

GOVERNMENT

INDUSTRY

- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
  - Complex logistics
  - On-boarding every user is expensive
  - Disruption to the banking industry

- Arguments from a privacy perspective for a direct CBDC:
  - Central banks are trustworthy on data privacy issues
  - Financial tracking rules are streamlined
  - Hard privacy doesn’t work well at this level

- Central Banks do not want to run a CBDC alone (a “direct CBDC”):
  - Complex logistics
  - On-boarding every user is expensive
  - Disruption to the banking industry

- Arguments from a privacy perspective <u>for</u> a direct CBDC:
  - Central banks are trustworthy on data privacy issues
  - Financial tracking rules are streamlined
  - Hard privacy doesn’t work well at this level

- Arguments from a privacy perspective <u>against</u> a direct CBDC:
  - Less consumer choice
  - Corruption within government

# Q

@PulpSpy