

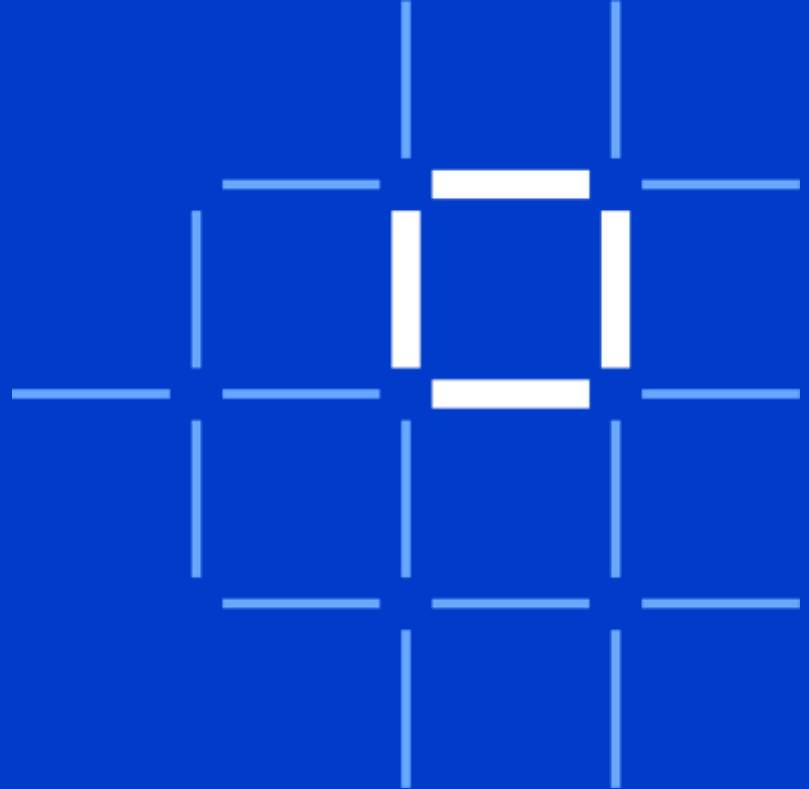
# CBDCs Promise and Risk:

Operationalizing CBDC's

Saket Sinha

Global Vice President – FSS Blockchain

2021



# FSS Industry has reached an inflection point



- A race is on across the globe
  - Industry is re-plumbing capital market processes
  - Addressable business with blockchain has significantly grown
  - FI's significantly up their spend on blockchain projects (CLS, We.Trade, ASX, Visa, BNPP, HSBC, Santander, MUFG)
- Emergence of low footprint business applications on blockchain at negligible maintenance cost on Cloud
  - Business is leading adoption of blockchain
- Blockchain has emerged as the top play for dramatically cutting operations cost and reducing risk

*BBVA launched Blockchain-Based Syndicated Loan platform with BNP Paribas and MUFG raises \$500M+ in syndicate loans for corporate clients to win banking tech innovation award*

*DBS launches supply chain finance blockchain for Chinese enterprises to target \$1.3T in financing gaps in the supply chain*

*Bank of Thailand issues first ever \$1.2B government bonds using IBM blockchain technology.*

*BNP Paribas Securities and Centotrenta launch a credit securitization management platform using IBM Blockchain Platform to address securitization servicing portfolio totaling €15.6 billion*

*JPMorgan, Citi, BNPParibas, Goldman Sachs reinvent settling forex transaction son IBM powered blockchain network at CLS*

*Bank of New York Mellon announces setting up digital custody solution for 1400+ institutional clients*

*HSBC Moves \$20 Billion in assets From Paper To Blockchain In One Of The Biggest Financial Deployments*

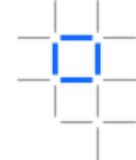
*Santander Settles Both Sides of a \$20 Million Bond Trade on Blockchain*

*Citi, Goldman Sachs Conduct First Blockchain Equity Swap On Blockchain that aims to revolutionize \$1Trillion equity swap market globally*

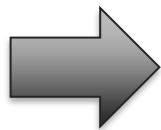
*Mitsubishi UFG (MUFG)'s banking arm launches its first blockchain-powered letter of credit along with participating institutions ING, Citigroup and BNP Paribas to reduce trade cycle time by 80%*

*OCC allows financial institutions to become digital custodians, issue their own Stablecoins and use public blockchain network for financial services*

# What's Changing Rapidly



\$2 Trillion



Cryptos

- Value Influx Via Derivatives Markets
- New Asset Class
- Value from Borrowing, Lending & Staking Cryptos
- Decentralized Finance
- New Capital Markets Infrastructure
- Upending Traditional Intermediaries

# Why are Central Banks Interested in CBDCs

## Objectives

## Challenges

### Currency Issuance and Management

*Minting, Printing & Quantitative Easing*

- **Issuance of national currency** as a direct proof of claim (i.e. cash) on Central Bank
- **Quantitative Easing** – Purchase of securities from commercial banks, increasing the monetary supply to encourage lending
- **Helicopter Money** – Direct relief payments to individuals

- **Seignorage** – Cost of printing physical money
- **Financial Inclusion** – Limited distribution avenues to the unbanked, most vulnerable population in a crisis
- **Capital Flight** – Commercial Banks investing in foreign or alternative markets rather than domestic businesses

### Monetary Stability

*Managing Interest & Exchange Rates*

- Managing **inflation** and setting **foreign exchange** rates
- **Currency Devaluation** – Lowering the exchange rate to boost exports and increase domestic consumption
- **Interest Rate Reduction** – adjusting the short-term interest rate to increase the availability and lower the cost of credit

- **Costly Imports** – increased cost of imports in domestic currency spurs inflation
- **Lack of faith** in Central Bank's commitment or in rebounding economy restrict lending practices

### Payment Clearinghouse

*Supporting RTGS and Cross-Border Trade*

- **Executing payments** between commercial banks
- **Automated Clearing House** – defers net settlement for batched payments between commercial banks on behalf of customers
- **Real-Time Gross Settlement** –executes clearing and settlement of payment between sender and receiver in seconds

- **RTGS Gridlock** – Payments delayed as banks await settlement of others to increase their individual liquidity
- **Outages** – lack of resilient, high availability network
- **Limited FX and Securities Settlement** – Reliance on commercial, correspondent banking and custodians

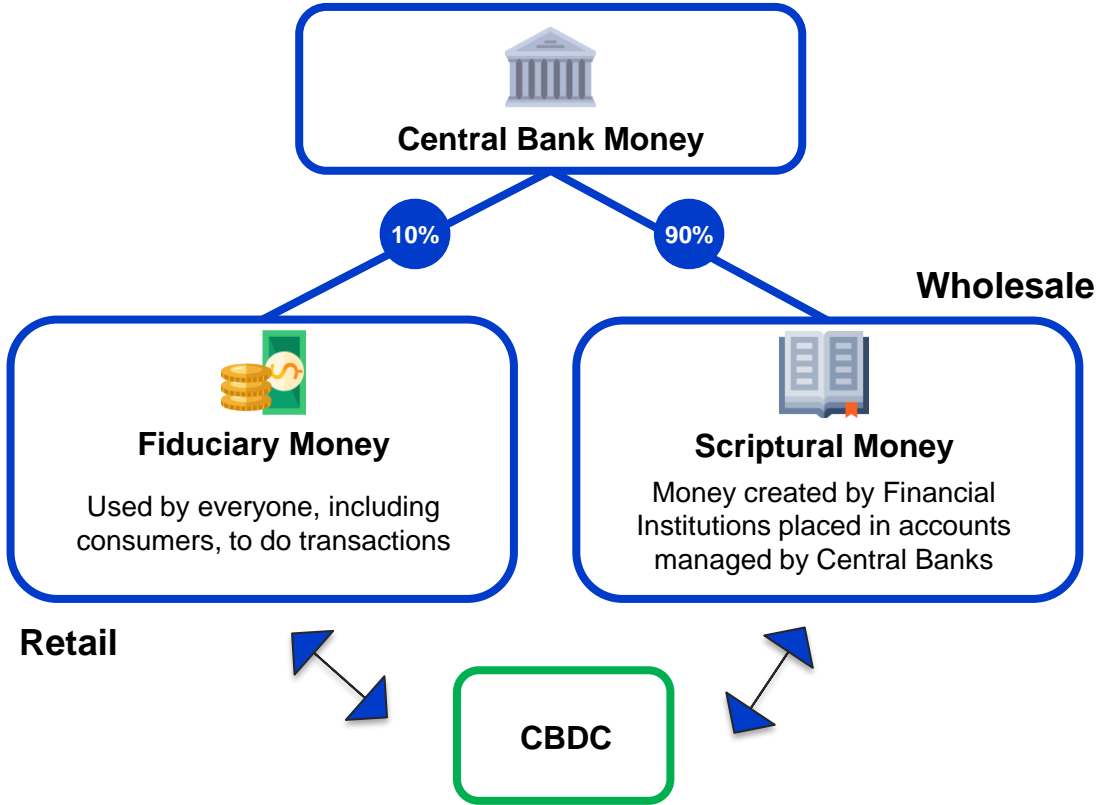
### Financial Stability & Bank Regulation

*Managing Reserves and Protecting Consumers*

- Holds deposits and serves as the **lender of last resort** to member banks
- Establishing **banking rules and regulations** (i.e. leverage ratio and liquidity coverage requirements)
- Safeguard stability and **protect consumers**

- **Lack of real-time oversight** into the M3 money and securities issued by Commercial Banks
- **Insufficient supervision** over new financial technology
- **Outdated Regulatory Frameworks** to make all of this new financial innovation work properly

# Central Banks Digital Currency



A CBDC may be defined as:

- a digital asset that **only the central bank** may issue or destroy,
- that is **traded at par against banknotes** and **reserves**,
- that is **available 24/7**,
- that may be used in **peer-to-peer transactions**,
- Is only issued by central banks
- Financial institutions hold accounts with central banks to access CBDC's
- Consumer bank account is not central bank money, it is a claim on the bank
- Consumers have the right though to convert their claim into cash

The primary reason for issuing a CBDC would be to offer a **perfectly liquid and safe payment instrument** that is adapted to technological changes.

# Aiming for the perfect world

## Sovereignty

- Competition from foreign digital currency whether private or public (i.e. Libra or Digital RMB)
- Monetary Policy hinges on the government's monopoly of the money supply

## Avoiding Parallel Economies

- Crypto and physical fund payments within the black market
- CBDC and the shrinkage of cash usage would shrink the the black market and other *under-the-table* payments

## Regulatory Standards

- Fast-moving startups, banks, and fintechs pose risks to stability and potential harm to consumers
- Better understanding of disruptive nature of new technology introduction into the market

## Risk Management & Mitigation

- Today, technology failure or collapse of a larger bank will stifle payments by smaller banks and new entrants
- Direct connectivity for NBFIs reduces reliance on potential points of failure

## Transparency

- Crypto and cash are virtually anonymous and untraceable
- CBDC allows for investigation suspicious activity and ability to trace tokens or account-based activity

## Liquidity

- More payments services providers could connect directly to the Central Bank
- Reduces concentration of liquidity on settlement of payments by tier I banks

# Central Banks Motivations With Blockchain

## Currency Issuance and Management

*Minting, Printing & Quantitative Easing*

### Digital Currency Issuance

- Provides an accessible, future-proof payment method
- Cuts seignorage costs
- Mitigates financial exclusion and risk created by private money
- Builds a direct path to helping local businesses and individuals in need

#### Why Now?

COVID-19 has spurred many governments to allocate funds directly to citizens and corporations, but the current distribution system excludes the un and under banked

## Monetary Stability

*Managing Interest & Exchange Rates*

### Atomic Settlement

- Allows securities transactions to be executed with finality
- Improves liquidity management and visibility of exposure to risk across financial market
- Integrates securities settlement across commercial bank infrastructure to remove counterparty risk

#### Why Now?

The uptake of domestic RTGS systems has outpaced the clearing systems of security transfers increasing the need for and cost of reconciliation

## Payment Clearinghouse

*Supporting RTGS and Cross-Border Trade*

### Payment Tokenization & Decentralization

- Streamline clearing and settlement
- Accelerates gridlock resolution
- Streamlines cross-border payments between key trading partners
- Minimizes single point-of-failure risks to stability through distributed network deployment

#### Why Now?

Demand for domestic payment modernization is on the rise, simultaneously increasing customer expectations for cross-border payments

## Financial Stability & Bank Regulation

*Managing Reserves and Protecting Consumers*




### FinTech Regulatory Sandboxes

- Controls and secures development of new technology
- Allows sufficient supervision for accelerated fintech innovation
- Provides space for analysis and evaluation of existing regulatory frameworks and next generations technologies

#### Why Now?

Startups, Banks, and FinTechs are moving faster to bring new value, and Central Banks need to keep up to maintain stability and protect consumers

# Central Banks: Current Activities

Stage	Discovery 	Experimental 	Operational 
<b>Goal</b>	<b>Understanding the challenges and available solutions</b>	<b>Evaluating the available solutions and their technical applicability and efficiency, regulatory implications, and security risks</b>	<b>Implementing available solutions to a limited or broader network.</b>
<b>Activities</b>	<ul style="list-style-type: none"> <li>• Digital Strategy Roadmap</li> <li>• Whitepapers / Discussion Papers</li> <li>• Call for Experiments</li> <li>• Protocol Survey</li> <li>• Consortia Building</li> </ul>	<ul style="list-style-type: none"> <li>• Pilots</li> <li>• Sandbox Deployments</li> <li>• Performance and Security Risk Assessment</li> <li>• Regulatory Framework</li> </ul>	<ul style="list-style-type: none"> <li>• Live Network Deployment</li> <li>• Disaster Recovery / High Availability Plan</li> <li>• Upgrades / Maintenance</li> </ul>
<b>Questions to ask</b>	<ul style="list-style-type: none"> <li>• Which Challenges are most important to tackle?</li> <li>• Which solutions would be most potent?</li> <li>• Which use cases are most important and when?</li> <li>• Which technologies (i.e. Protocol, cloud, key management, etc.) are best fitted for this context?</li> <li>• What are the macroeconomic implications of this solution?</li> <li>• What are the regulatory constraints and considerations for implementation?</li> <li>• Who could be involved in this new network?</li> </ul>	<ul style="list-style-type: none"> <li>• Which use cases are prioritized?</li> <li>• How effective is the solution in practice?</li> <li>• How can the solution integrate with existing systems and networks?</li> <li>• Who should be involved and responsible for activities in a new solution?</li> <li>• What is the role of the Central Bank in the operation of the solution?</li> <li>• Is this targeted towards institutions or individuals?</li> <li>• Will this impact international systems or just domestic ones?</li> <li>• Is privacy and confidentiality managed at the system, account, or token-level?</li> <li>• What use cases need to be prioritized?</li> <li>• Which metrics are most important for measuring success (i.e. speed, resilience, security, usage, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• What training is needed to support a new network?</li> <li>• How will upgrades be doled out in conventional or DLT, node-based infrastructure?</li> <li>• What are the regulatory reporting mechanisms to ensure compliance in a new network?</li> <li>• How will financial inclusion be ensured along transformation journey?</li> </ul>



# What Are Central Banks Most Worried About

## Regulatory, Policy and / or GRC Gaps

- Tokenized clearing and settlement processes
- Digital asset custody / digital wallets
- Automated GRC
- Real-time payments and transactions processing
- Financial Crimes

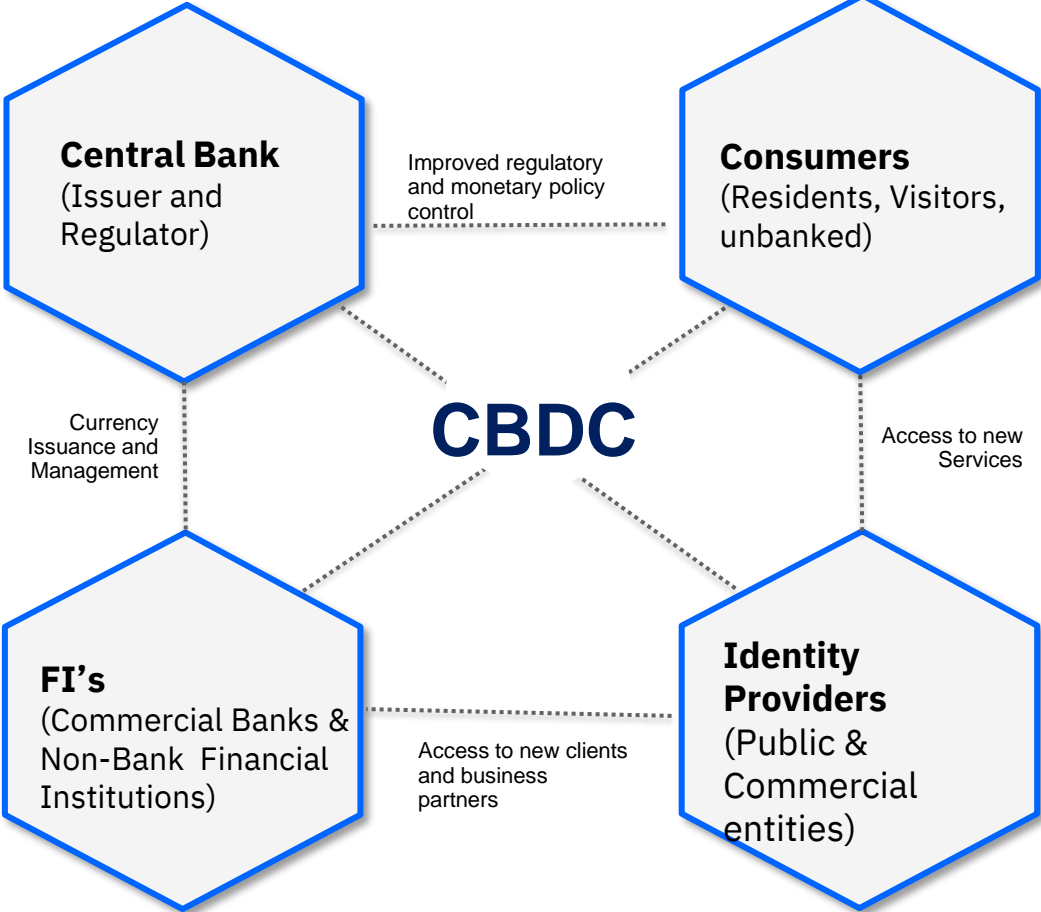
## Technology Gaps

- Security
- Real-time Visibility and balances
- Surveillance
- Cash Flow forecasting
- Infrastructure – Public vs. Private Networks

## Fiduciary Gaps

- Market Consensus
- Asset Value Protection
- Economic Threat – Concentration, Run on CBDCs

# Key Stakeholders



- *Impact on Monetary Policy*
- *Improve financial surveillance*
- *Faster transmission of simulation packages*
- *Increased operational responsibility, risks?*

**Central Bank**  
(Issuer and Regulator)

Improved regulatory and monetary policy control

**Consumers**  
(Residents, Visitors, unbanked)

- *Need seamless access, be able to pay goods and services with least friction*
- *May not have a bank account in the country*
- *Concerned about greater scrutiny and invasion of personal privacy*

Currency Issuance and Management

**CBDC**

Access to new Services

- *Concern about disintermediation with CBDC*
- *Need to re-evaluate value/offerings provided by Commercial Banks*
- *Potential to capture new client by offering differentiated service*

**FI's**  
(Commercial Banks & Non-Bank Financial Institutions)

Access to new clients and business partners

**Identity Providers**  
(Public & Commercial entities)

- *Provide mechanism to establish identity of individuals and corporates in the country.*
- *Provide mechanism to establish identity of individuals and corporates for a given service.*
- *Not accountable for actual service performed*

# Key Considerations

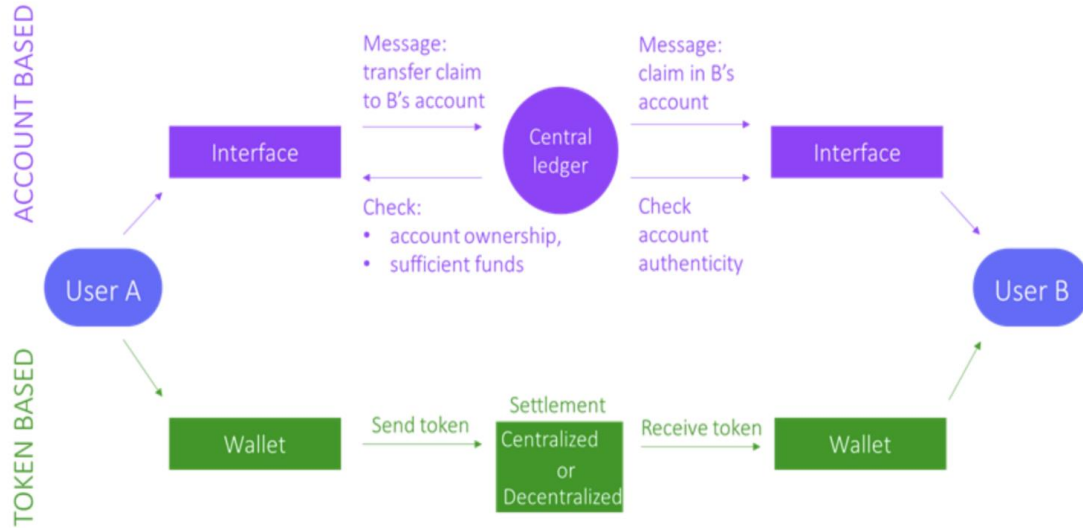


**Business Model**

**Technology**

**Operational**

# Business Model: Account Type

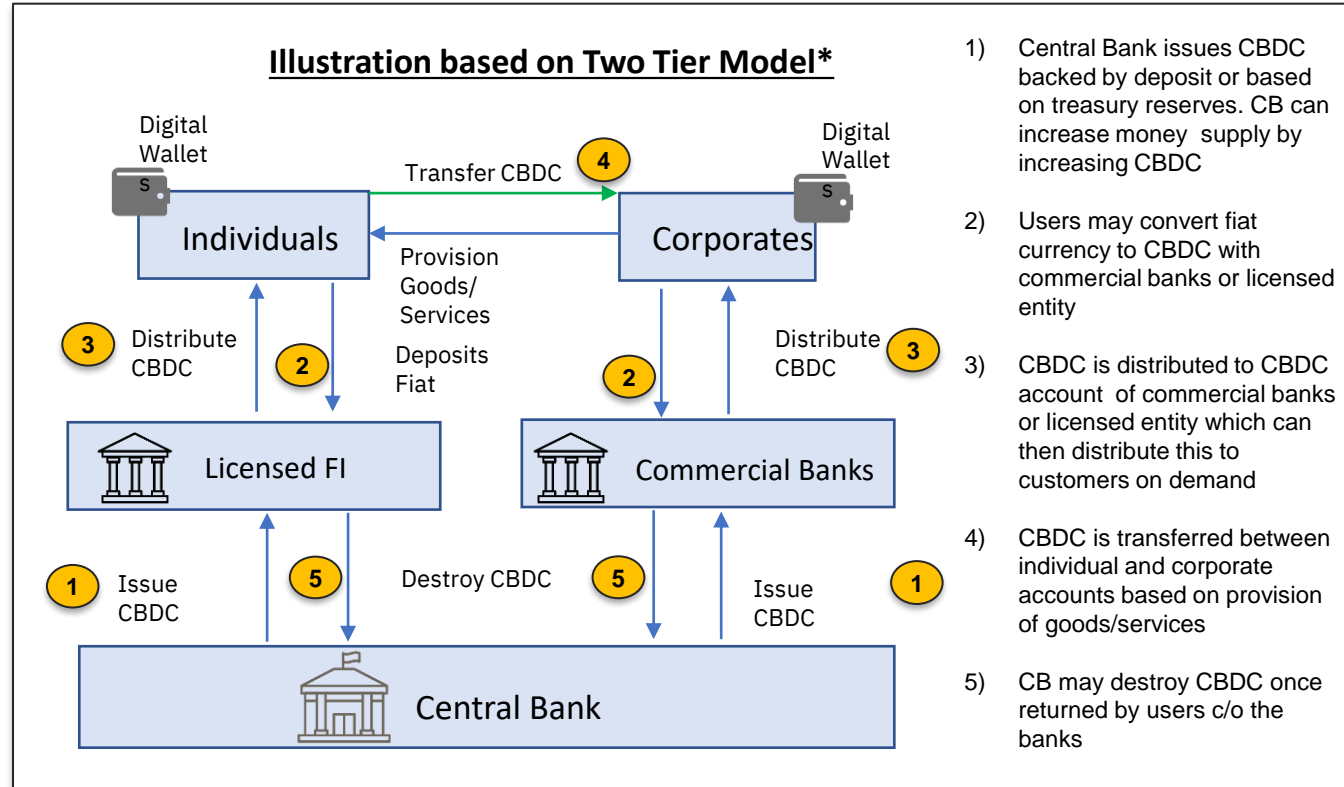


Source: IMF

- **Account-based**
  - Adaptable
  - Secure value storage
  - Suited to payments of any size
  - Dependent on contact with a third party
  - Close substitute for bank deposits
- **Token-based**
  - Local and independent of communication with a third party
  - Not traced or recorded in a central database
  - Money is lost if wallet or payment instrument is lost or damaged or stolen
  - More closely aligns with cash

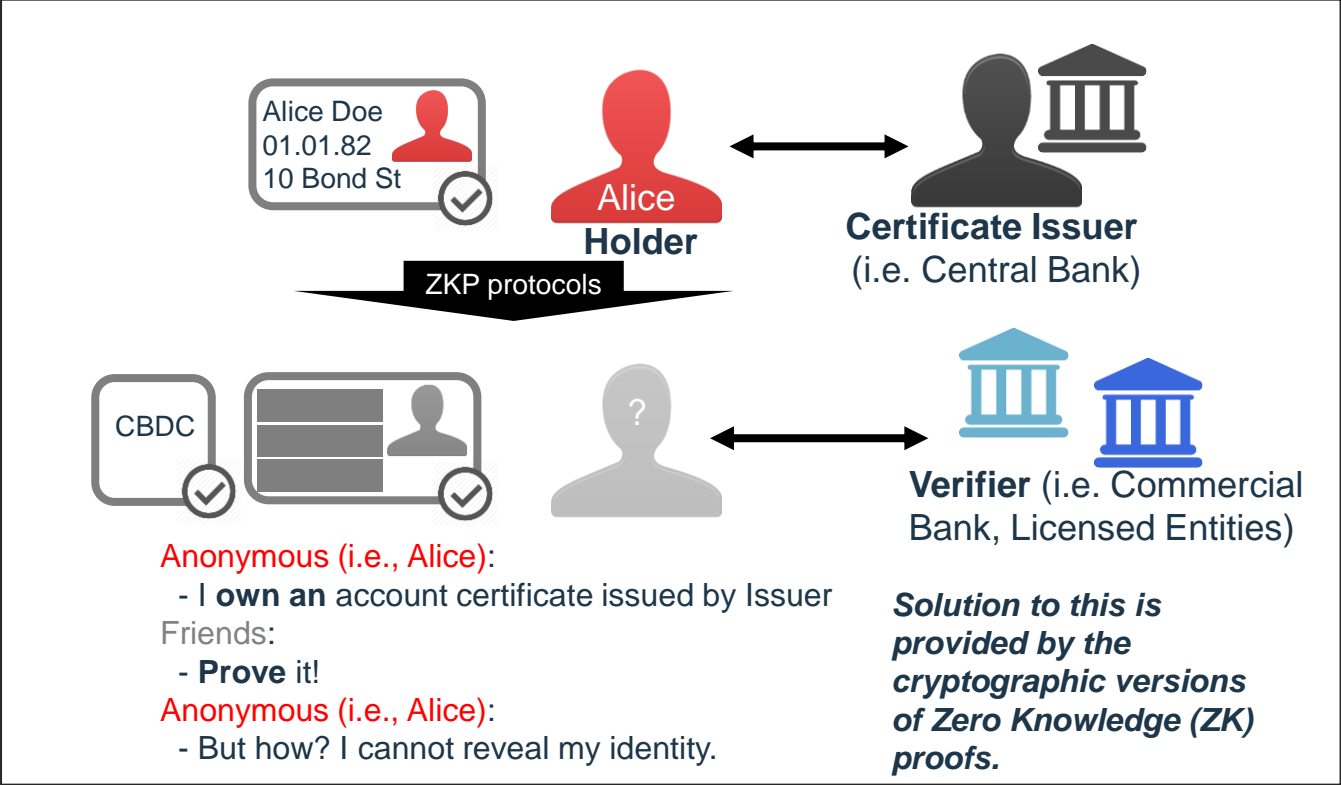
# Business Model: Distribution

- Flexibility to support single and two tier distribution model\*
- Proposed model leverages existing distribution mechanism available through payment network of commercial bank and other non-bank FIs.
- Consumers will interact with existing payment providers rather than go direct to central banks to receive or return CBDC.
- Disbursement of government subsidies will go direct to consumer's accounts.



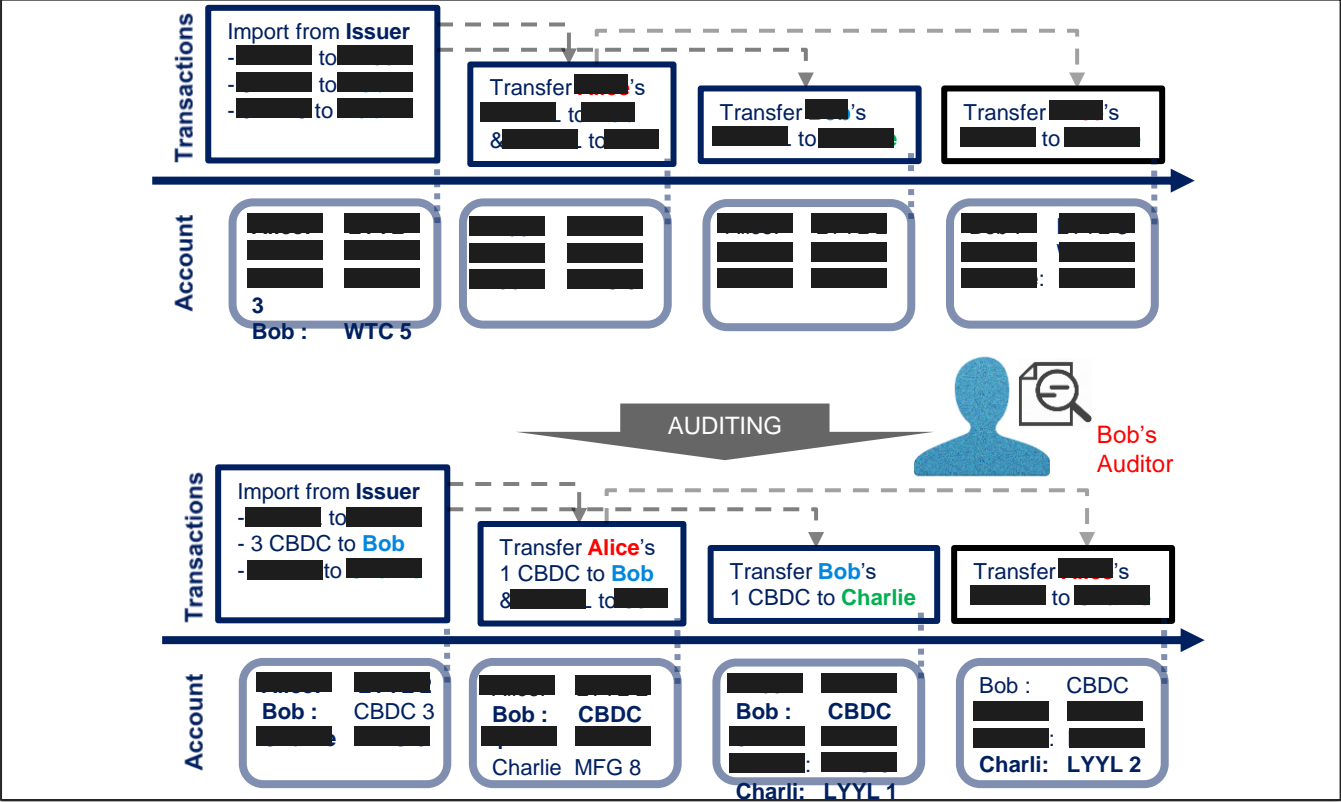
# Business Model: Coverage

- CBDC is accessible to different set of entities and consumers including existing accounts with licensed entities
- No lock-in to a single payments provider or commercial bank.
- Possibility of incorporating other identity providers, including existing national identity infrastructure



# Business Model: Privacy

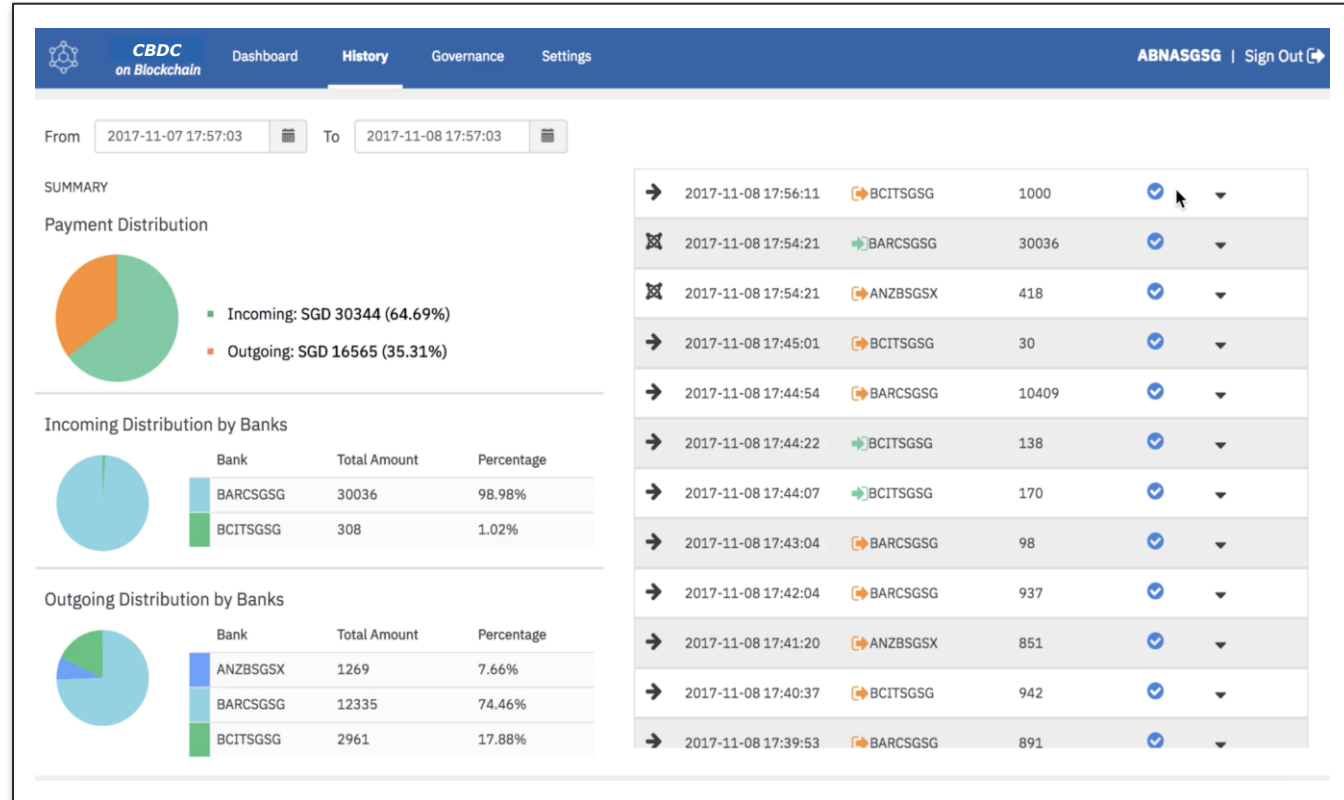
- Full privacy model include concealing Transaction graph and Transaction detail with complete anonymity. Trade-off performance. A Partial privacy model offers greater performance
- Auditability in privacy-preserving asset management can be served with Zero-Knowledge proofs.
- On a per user-level: auditors bound to a user are guaranteed unconditional access to that user's transaction details



# Business Model: Control

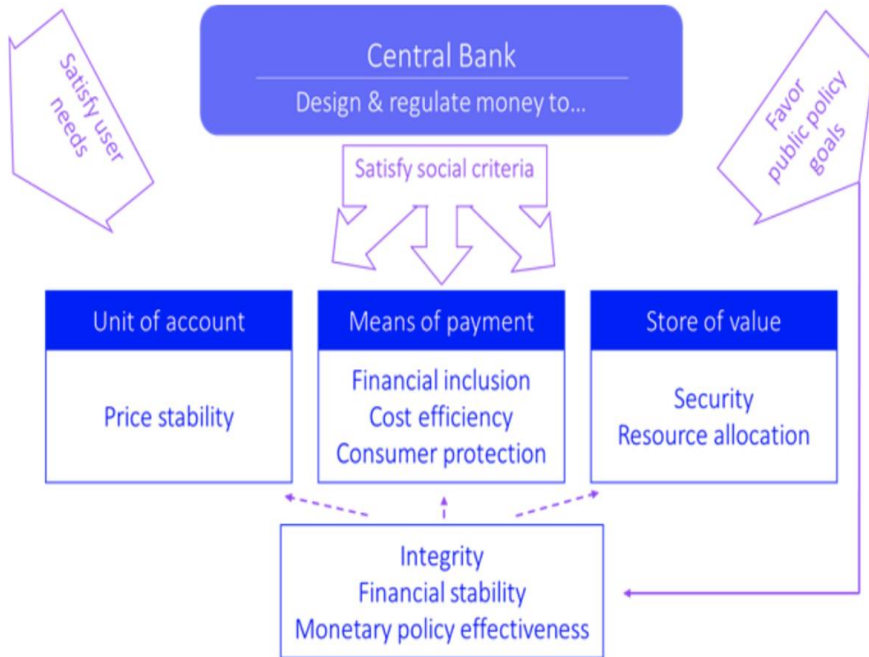
Allow Central Bank to oversee system and set CBDC supply.

- Central Bank could put in place, circuit breakers to prevent activities that could undermine the stability of the financial infrastructure
- Commercial Banks still be required to retain deposits with Central Bank per reserve requirements.
- CBDC accounts are negative or zero interest bearing. Consumers have flexibility to convert to interest bearing accounts held with Commercial Banks or other Financial Institutions





# Business Model: Social



- **Unit of Account**

- The currency should be stable to allow determination of nominal wages and prices.
- In order to mitigate inflationary impacts, consideration should be given to an interest rate on the CBDC that can be adjusted upwards or downwards as needed;
- The real value of the CBDC should remain stable over time, as measured against a general index of consumer prices.

- **Store of Value**

- Should bear same interest rate as other risk-free assets

- **Medium of Exchange**

- The CBDC should be Legal Tender: the government should mandate its acceptance for all payments to both private and public sector, including the payment of taxes.
- The CBDC should be universally accessible: any household or firm may hold funds in a CBDC account
- Transactions should be instant and near costless (similar to the movement of funds between accounts in a single commercial bank)
- Must support anonymous transactions
- There should be sufficient protection against fraud, theft, and loss for consumers;

# Business Model: Interaction

## Three distinct types of interaction models

1. Only Financial Institutions interact with the CBDC
2. The CBDC is available to Banks and NBFIs
3. The CBDC is available to the entire economy to interact with it

Central Banks

FI's / Banks

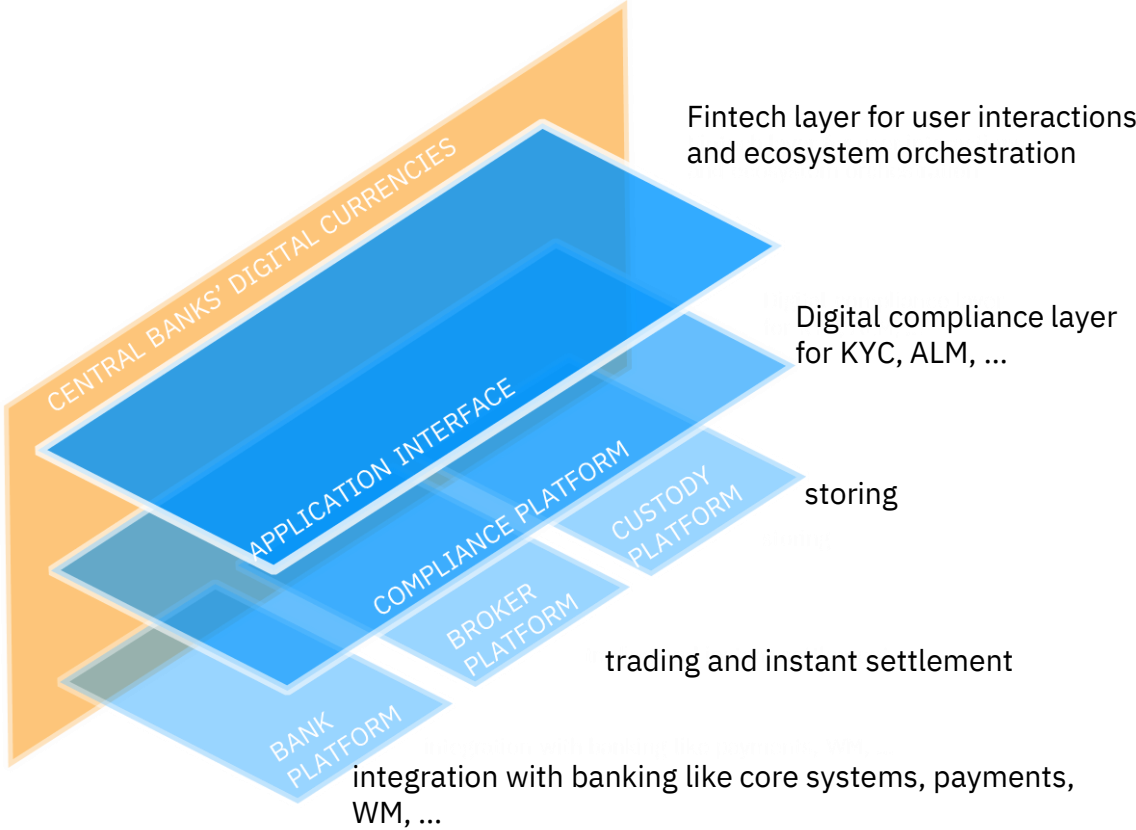
NBFI's

CBDC  
Exchange

# Technology Considerations

1. Ecosystem Participation
2. Decentralized credentials
3. Interop with digital and crypto Currencies
4. Integration
5. User Managed Wallets
6. Offline payments
7. Privacy

# Technology Considerations: Ecosystem Participation



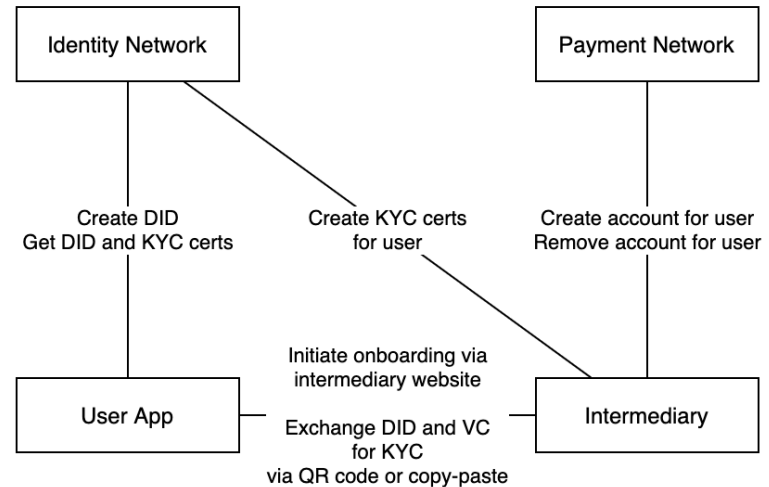
# Technology Considerations: Credentials

## Motivation:

- Enable KYC, AML, and CFT work to be performed by private-sector intermediaries with trust
  - Private sector might prefer to selectively reveal their customer information
  - Leverage on existing customer relationships and business processes
- Decentralize/Distribute the work of onboarding

## Technology Readiness:

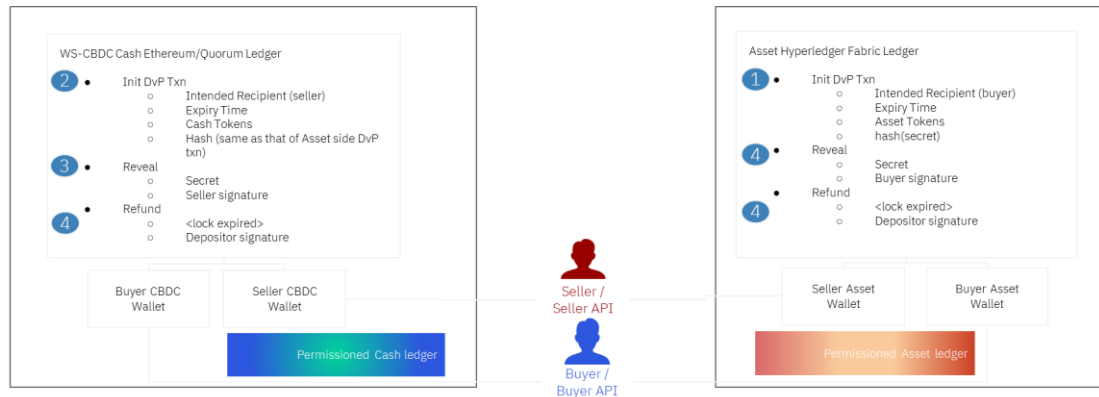
- IBM Verify Credentials (running on Hyperledger Indy) already works for identity and proofs/verifiable-claims
- KYC does not need high throughput (due to digital certs and non-interactive proofs)



# Technology Considerations: Interoperability

- ERC20 interface
- Cross-chain atomic swaps (e.g. HTLC support)
- Set interop standards for non-crypto digital currencies

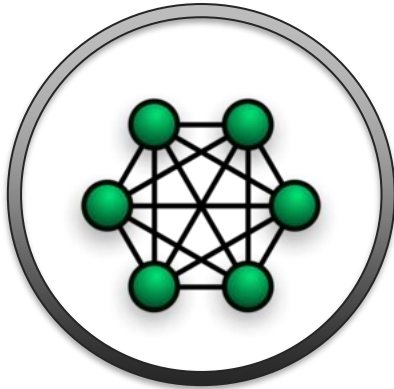
## Atomic Swap Example



### Notes:

- 0. Seller owns asset, buyer owns cash, with both owning accounts in both ledgers
- 1. Buyer & seller agree to trade. Seller creates secret, hashes secret, deposits asset for buyer on asset ledger, notifies buyer
- 2. Buyer deposits cash on cash ledger and notifies seller
- 3a. Seller calls HTLC on cash ledger with secret, HTLC smart contract performs validations, releases cash and reveals secret
- 3b. Buyer using revealed secret, calls HTLC on asset ledger, HTLC smart contract performs validations and releases token(s) to buyers
- 4. Buyer fails to deposit cash on time, seller reveals password upon timer expiry to HTLC contract and reclaims deposited asset back

# Technology Considerations: Integration



## Full Mesh Connectivity

Unlike traditional RTGS systems, DLT needs full mesh connectivity between participants.



## Access to Common Services

Commercial banks will need access to some common services. E.g. CA services or blockchain technology specific (notary, ordering etc.)



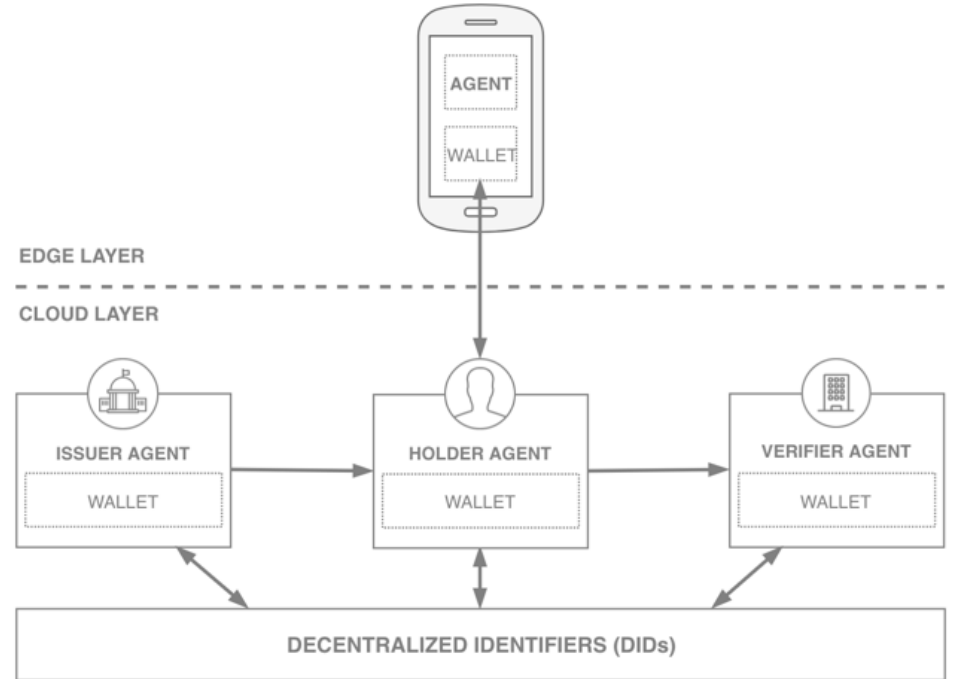
## Access to Core Banking

DLT will need to be hooked up to system of record using manual processes or online integration.

# Technology Considerations: Wallets

- User wallet for storing proof of identity can be stored on smart phones
- User wallet not bound to a bank account
- Allows the unbanked to hold and use CBDC even without a bank account
- Optionally, banks can also store user wallets for them

## User Managed Wallets



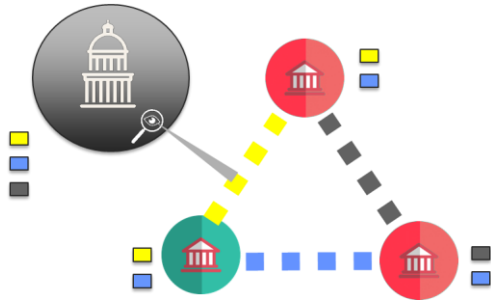


# Technology Considerations: Offline Payments

- Technically a separate system
- Traditional techniques
  - Electronic cash devices
  - Store and forward
  - Does not require special support on the payment network
  - Need regulation, legal enforcement, fraud management etc.
- New techniques from blockchain:
  - Micro-payment-channels (This requires special support from the payment network) (this is same technique as lightning network)

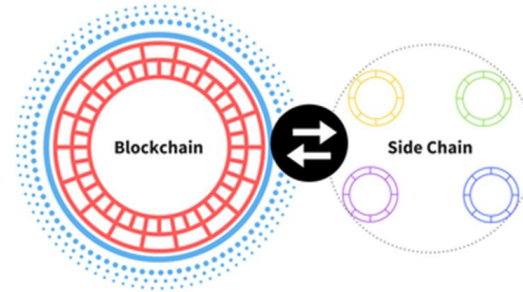
# Technology Considerations: Privacy

## Private Channels & Subledgers



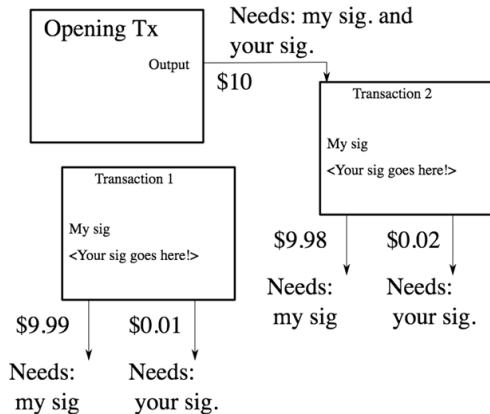
- A subledger cryptographically linked with the main ledger.
- A side channel for participants to perform private transactions.
- Supports auditing of private channels.

## Sidechains



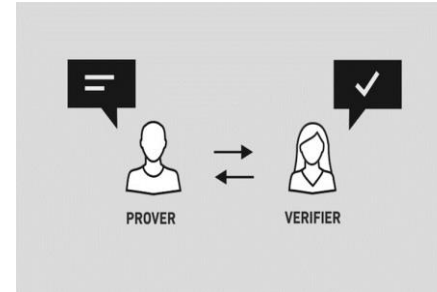
Allows assets to be moved across ledgers or sub-ledgers in a reliable way that avoids double spends. The sidechain is connected to the main chain with the two-way peg.  
Example: *Liquid* sidechain by Blockstream

## Lightning Network



- Part of layer 2 payment protocol "Lightning network" that operates on bitcoin.
- Two participants can commit funds on the main blockchain and exchange transactions peer to peer on the channel.
- Option of closing a channel either consensually or on detection of fraud without any loss for an honest party.

## Zero Knowledge Proof



Allows prover to prove to verifier that a statement is true, without revealing any information beyond validity of the statement itself

# Operational Considerations

A central bank can consider different operating model each with its own pros and cons

## Operating Models

### Direct Model

- CBDC is a claim on the central bank
- KYC and onboarding is done by Central bank or designated intermediaries
- Central bank handles retail and wholesale payments

### Indirect Model

- CBDC is a claim on intermediaries
- KYC and onboarding is done by designated intermediaries
- Intermediaries handles retail payments
- Central bank handles wholesale payments

### Hybrid Model

- CBDC is a claim on central banks
- KYC and onboarding is done by designated intermediaries
- Central bank handles wholesale payments and periodically balances retail payments

## Pros

- Central bank has complete control
- Controlled introduction
- Faster penetration of market
- Technical and infrastructure independence
- Public - Private partnership
- Share the burden

## Cons

- Infrastructure and technical burden
- Less control
- Responsibility to safeguard intermediaries
- Time consuming
- Contradicting business priorities of for profit and for public service

# Operational Considerations

**Careful planning backed by legal, regulatory framework and policies are needed to successfully launch retail CBDC's**

## Intrinsic Value

- Fiscal impact on monetary policies
- New money or replaceable money
- Backing of fiat equivalent
- Impact on inflation
- Preserving the value against fluctuations in exchange rate of local currency
- Exchange from or into fiat value
- Guarantee of intrinsic value
- Insurance for preserving intrinsic value

## Purpose & Adoption

### Purpose

- Fiscal transparency
- Traceability
- Better control of fiscal stimulus
- Curbing parallel economy
- Taxation revenue
- Efficiency in movement of money
- Towards digitization

### Adoption

- Limited experiment
- Transactional value based
- Purpose based
- Mass adoption

## Identity & Ownership

- KYC and onboarding
- Account and ownership tie in
- Account vs. Token-based models
- Transaction recording and verification
- Public and private key infrastructure
- AML framework
- Strict vs Third-party Transaction Visibility

## Architecture

### Design

- Centralized databased vs. Distributed ledger technologies (DLT's)
- Permission and permissionless DLT's
- Direct accounts vs. Tokens

### Security

- Secured value of the digital currency
- Tamper proof, fraud resistant
- Digital key safeguarding
- Traceability
- Custody and vaults for both digital currency and fiat equivalent backing

### Infrastructure

- Technical infrastructure resiliency, scalability, availability
- Infrastructure security, Denial of service attacks
- Disaster recovery and Failproof rollback capabilities
- 24 X 7 operations
- Disaster recovery

## Interoperability

- Interoperability with existing payments networks
- Co-existence of other payment mechanism with retail CBDC
- Interchange and exchange
- Cross border payments
- Economic integration across region and globe
- Asset Fungibility

# Operational Considerations

	Security	Technical & Performance	Regulatory	Economic
Risks	<ul style="list-style-type: none"> <li>• Consensus loopholes</li> <li>• External Breaches</li> <li>• Internal Bad Actors</li> </ul>	<ul style="list-style-type: none"> <li>• Capacity Bottlenecks</li> <li>• Outages</li> <li>• Slowdowns</li> <li>• Critical Bugs</li> <li>• Complexity &amp; Interoperability</li> <li>• Off-line Transaction Redundancy</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of Traceability</li> <li>• New Actors and Activities</li> <li>• GDPR &amp; CPA / Privacy</li> <li>• Financial Exclusion</li> </ul>	<ul style="list-style-type: none"> <li>• Disrupting the Banks &amp; Credit Industry</li> <li>• Stricter Limits on Foreign Cash</li> <li>• Runs on Cash</li> <li>• Lack of Transparency to system shocks</li> </ul>
Starting Considerations	<ul style="list-style-type: none"> <li>• Public vs. Private Protocol</li> <li>• Public vs. Private Cloud</li> <li>• Application vs. Ledger Transaction recording</li> <li>• Separation of Duties &amp; Cybersecurity Assets</li> </ul>	<ul style="list-style-type: none"> <li>• Scope of Decentralization</li> <li>• Cloud Architecture</li> <li>• High Availability/ Disaster Recovery Plan</li> <li>• Clustering</li> <li>• Programmability and Extensibility</li> <li>• Offline Transactions</li> </ul>	<ul style="list-style-type: none"> <li>• Account vs. Token-Based Networks</li> <li>• Strict vs Third-party Transaction Visibility</li> <li>• Asset Fungibility &amp; Use case specificity</li> <li>• Data-based Analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Segregation of Activity</li> <li>• Renumeration vs. Zero-interest</li> <li>• Multi-Tier Platform vs. Direct Retail</li> <li>• Limits in Volume or Access</li> <li>• Domestic vs. International</li> </ul>

# Operational Roadmap



## Central Bank Digital Currency (CBDC) Strategy Advisory

- Protocol Assessment
- Security Assessment
- Business Value Assessment
- Use Case Selection
- Network Governance Model
- Business Requirements
- Regulatory Framework
- Economic Risk Indicators
- Design Workshops
- Post-Build Evaluation

### CBDC Network Deployment

- Protocol Selection
- Network Architecture
- Network Security Framework
- High Availability / Disaster Recovery Program
- Sandbox, Test Network, Production Network Environment
- Cloud or On-Prem Deployment

### CBDC Application Development

- Application Security Framework
- Application Architecture
- Testing Scripts & Release Plan
- Agile Development
- Performance Optimization & Testing
- Security Testing & Tool Selection
- Risk Analytics Instrumentation
- Cloud Infrastructure

### CBDC Operations

- Maintenance
- Security Testing & Resolution
- Back Office Operations
- Vulnerability Testing
- Issue Management & Resolution

- Digital Currency Issuance
- Atomic Security Settlement
- Real Time Payments Clearinghouse
- Fintech Regulatory Sandboxes

Q&A