Digital Rial: Progress and Challenges
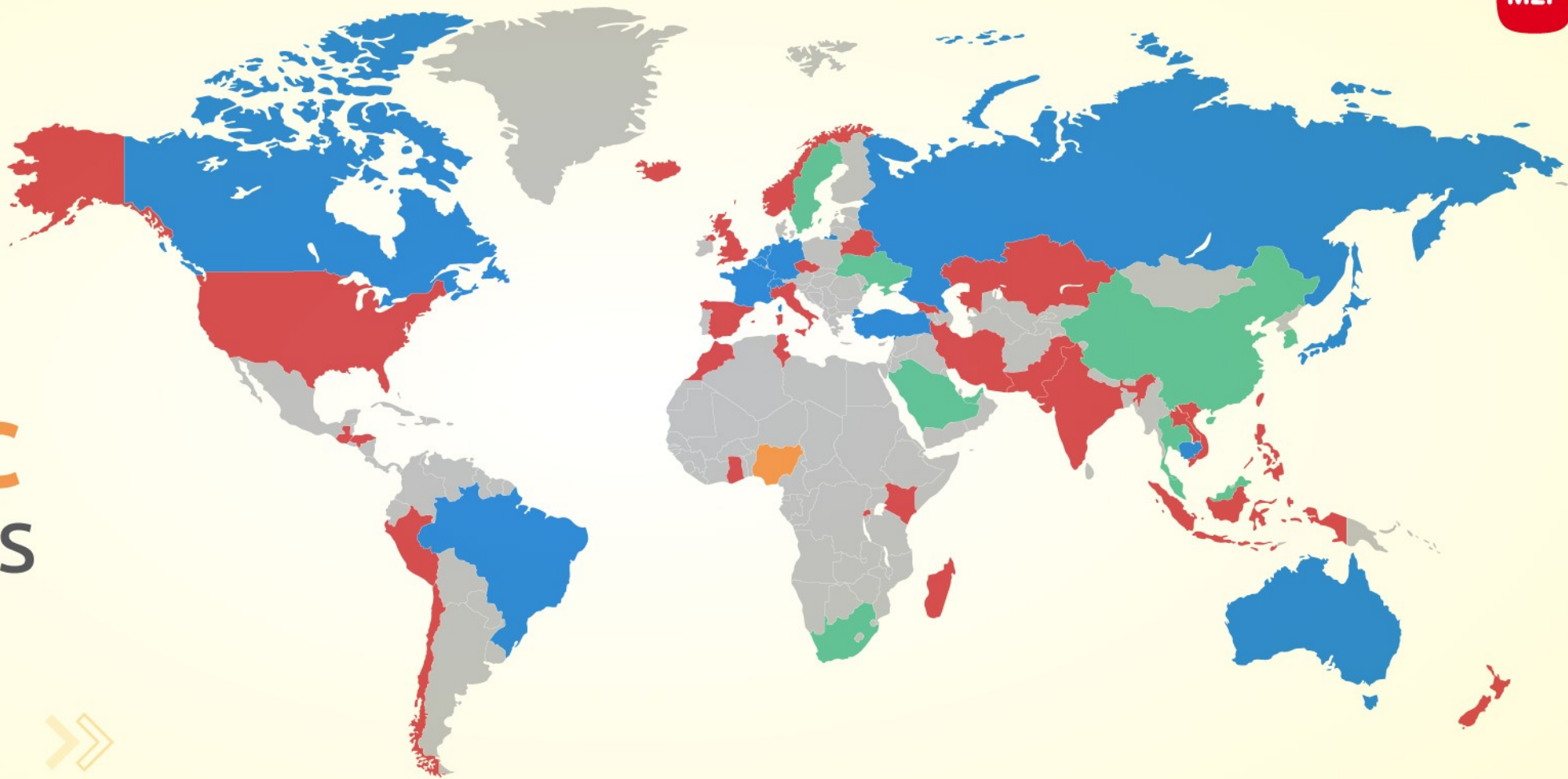
Amir Abbas Emami
Blockchain Economy Researcher

CBDC Status

Development | Launched | Pilot | Research

CBDC's combine attributes of traditional "fiat" currencies and cryptocurrencies

Traditional **Fiat** ← → Traditional **Crypto**

Attribute	Central Bank Notes (Cash)	Central Bank Reserves	Deposits	CBDC	USDC (Stablecoin)	Diem (Stablecoin)	Bitcoin	Ether
Central Bank Liability	✔	✔	✖	✔	✖	✖	✖	✖
Legal Tender	✔	✔	✖	✔	✖	✖	✖	✖
Convertible at par to Reserves/ bank notes	✔	✔	✔	✔	🟡	✖	✖	✖
Interest bearing	✖	✔	✔	Depends	✖	✖	✖	✖
Electronic	✖	✖	✔		✔	✔	✔	✔
Universally accessible (e.g., Anyone with digital signature can accecss)	✔	✖	✔	Depends	✔	✔	✔	✔
Token (Ownership tied to digital signature) or account-based (Ownership tied to identity)	Token	Account	Account	Depends	Token	Token	Token	Token

✔ Fit   ✖ Not a fit   🟡 Partial Fit

M2P

Differences between
Digital currency & Cryptocurrency

M2P

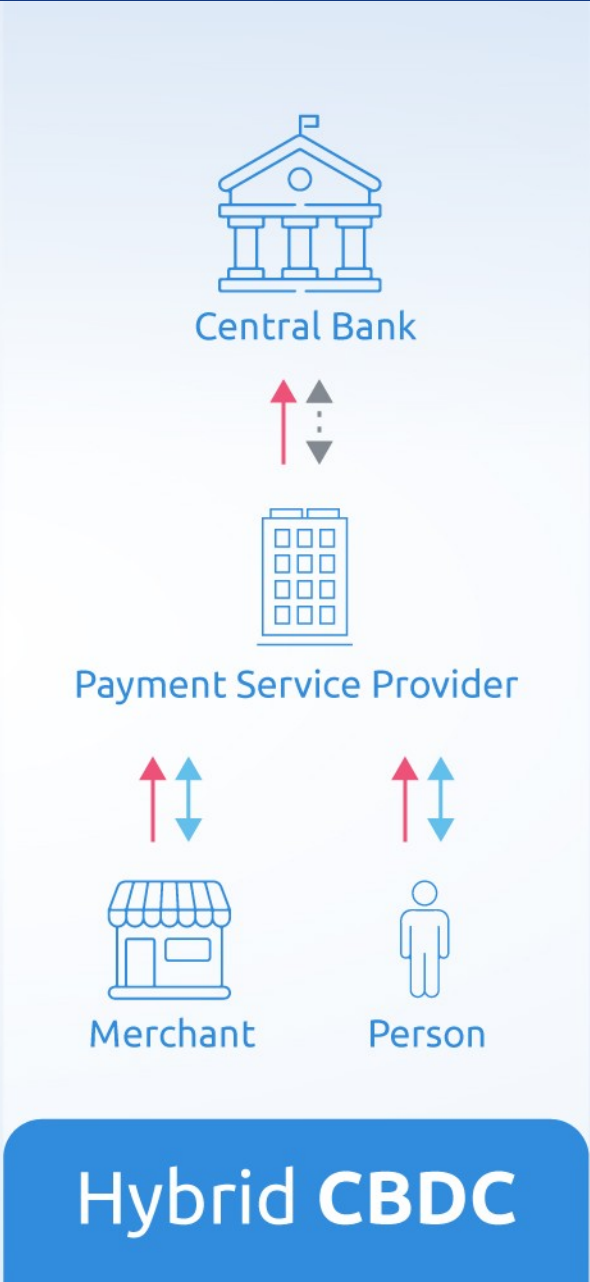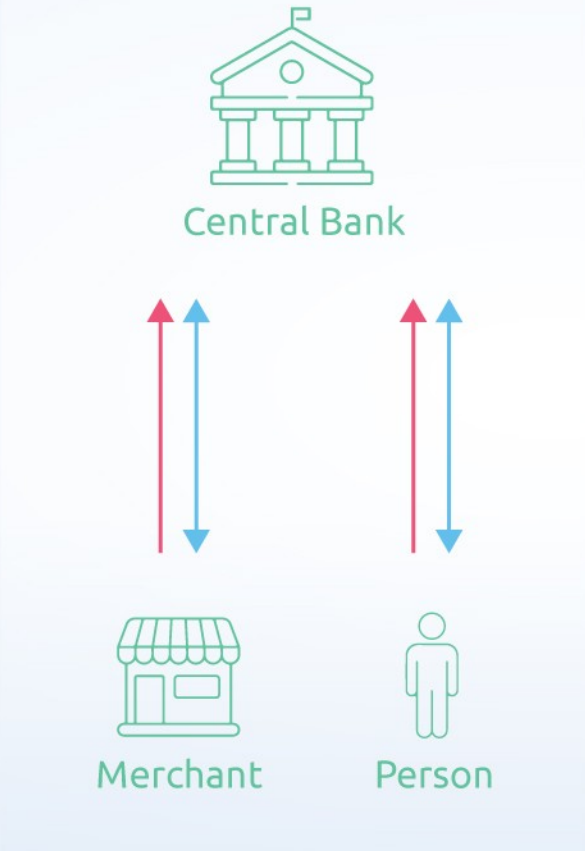|	TL/DR	
Digital currency is the electronic form of fiat money that can be used in contactless transactions.		Cryptocurrency is a store of value that is secured by encryption.
Digital currency is regulated by central authority (RBI for India).	**Regulation**	Cryptocurrency is decentralized and unregulated.
Digital currency rates are stable, and currencies are globally accepted.	**Stability & usage**	Cryptocurrency rates and highly volatile, and digital coins are not widely accepted yet.
Digital currency transactions are only known to the sender, receiver, and the bank.	**Who gets to know about the transactions?**	Cryptocurrency transactions are publicly available on a decentralized ledger.
Digital currency needs strong password to protect digital wallets, banking apps, credit, debit cards.	**Encryption & blockchain usage**	Cryptocurrency is secured by encryption.
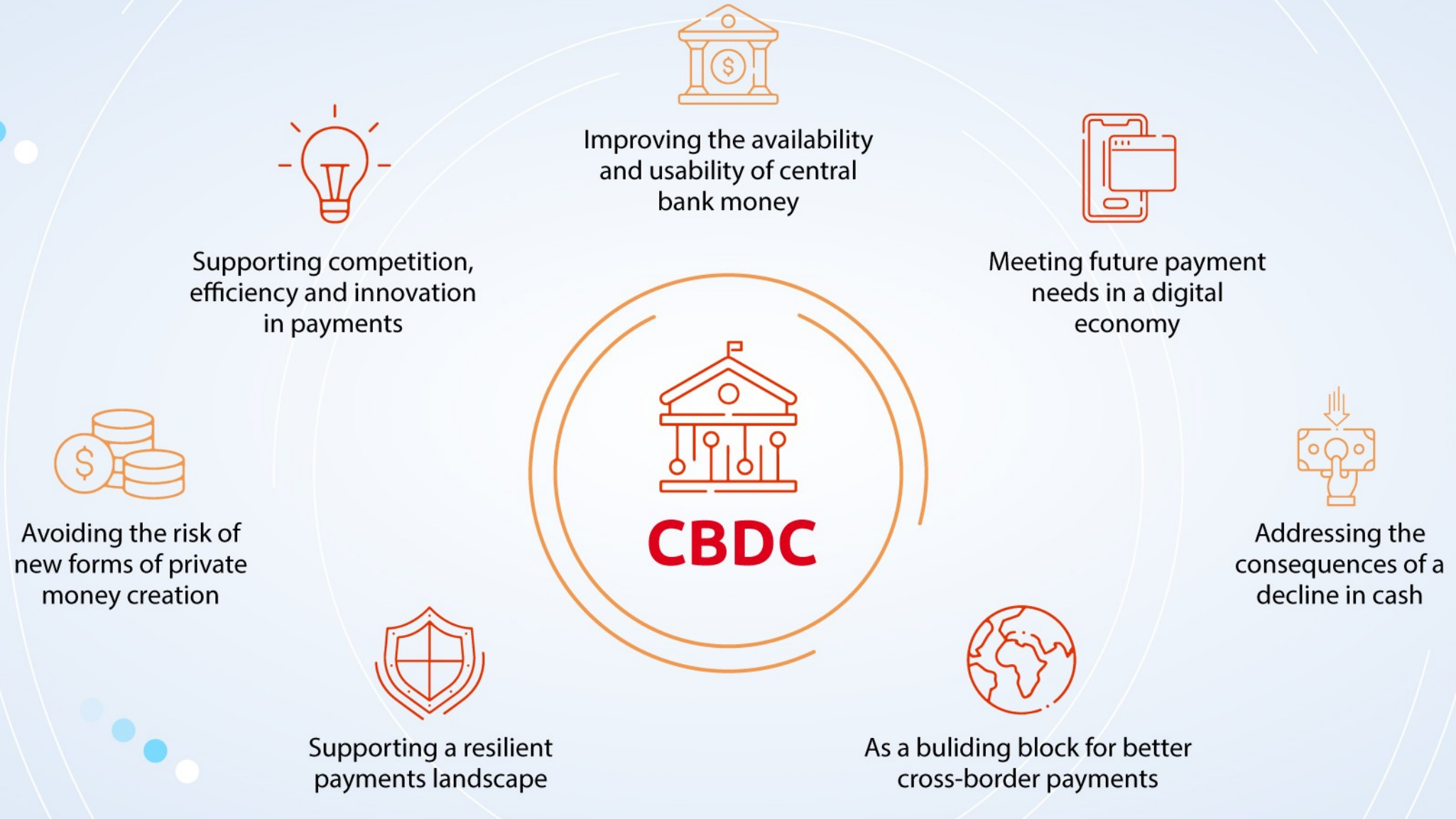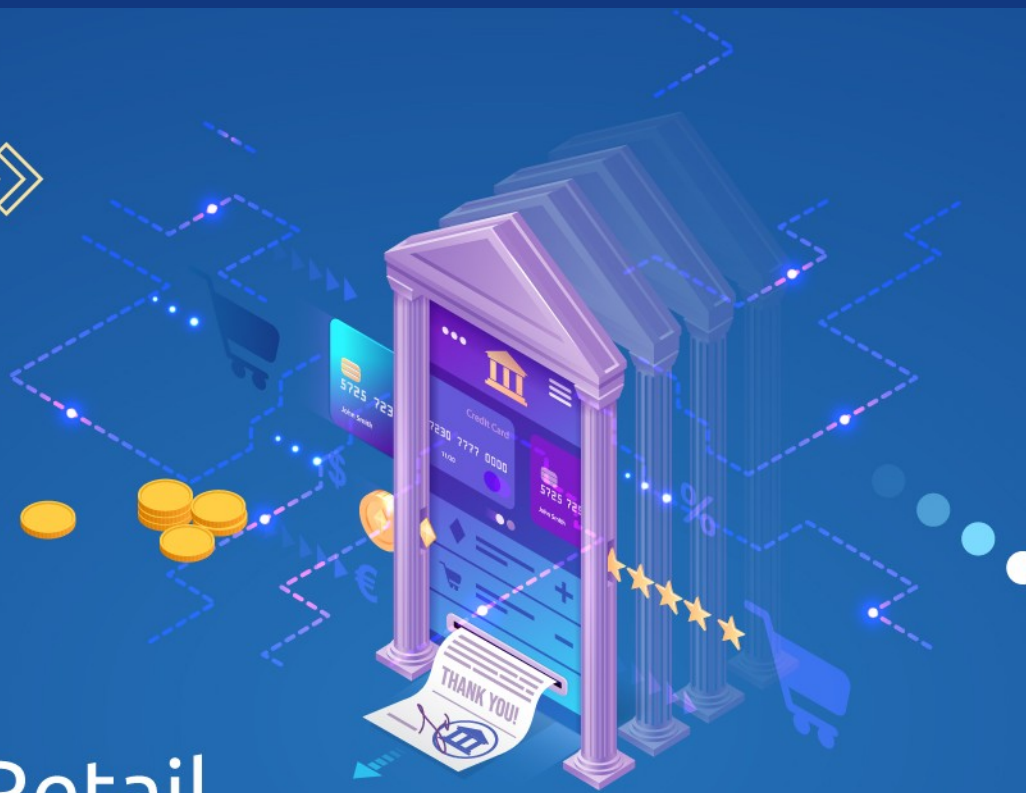
Retail CBDC

Used by individuals to make purchases at stores or even to one another. Simply put, CBDC's can be viewed as a digital form of physical cash, like a digital banknote.

Wholesale CBDC

These are more for financial institutions like banks. Such CBDC's can be used to settle interbank payments and transactions, like electronic bank reserves held at the Central Bank.

Indirect CBDC

Central Bank

Commercial Bank

Merchant   Person

Direct CBDC

Central Bank

Merchant   Person

Hybrid CBDC

Central Bank

Payment Service Provider

Merchant   Person

M2P

Legend

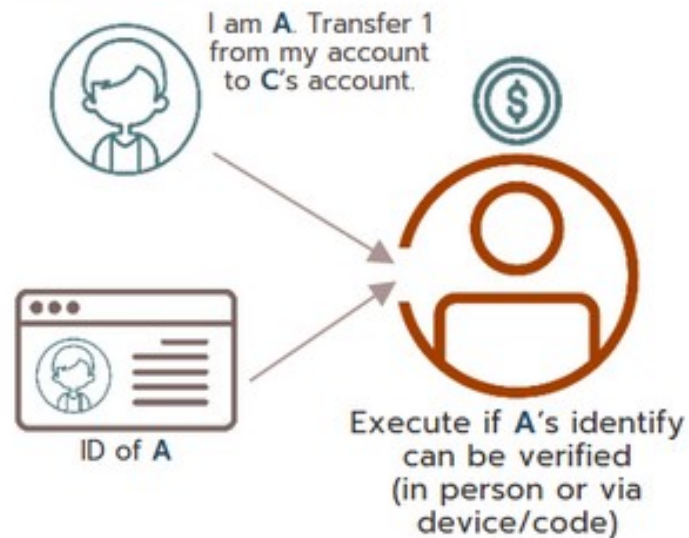Legal Claim

Direct Payment Communications

Deferred Payment Communications

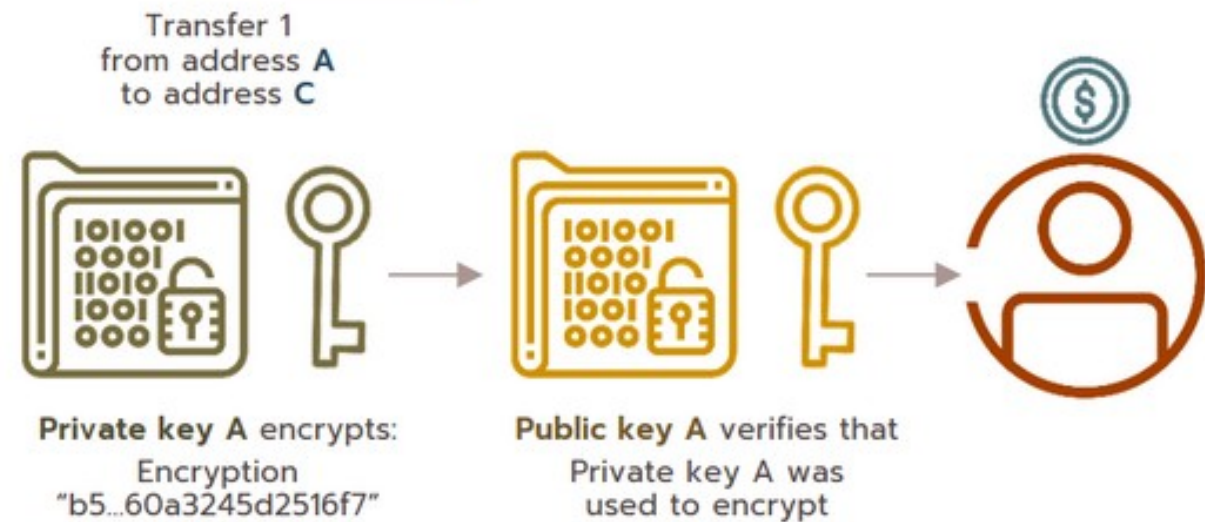# Here are the distinct highlights of the three types of architecture of CBDC

Criteria	Indirect CBDC	Direct CBDC	Hybrid CBDC
Liability	CBDC issuers or intermediaries take on the liability.	Central bank takes on liability.	Central bank takes on liability.
Issuing CBDC	Intermediaries issue CBDC to the public.	Central bank is responsible for issuing CBDC.	Central bank issues the CBDC while intermediaries take care of CBDC distribution to the public.
Operational Roles	CBDC issuers take care of KYC procedures and management of retail payments.	Central banks are responsible for the onboarding and management of retail payments.	Intermediaries take care of KYC and retail payments.
Recordkeeping	CBDC issuers maintain records of retail balance.	Central banks maintain records of retail balance.	Central banks and intermediaries maintain records of retail balance.

Account-based access compared with token-based access

Accounts: "I am, therefore I own"

I am A. Transfer 1 from my account to C's account.

ID of A

Execute if A's identify can be verified (in person or via device/code)

Digital tokens: "I know, therefore I own"

Transfer 1 from address A to address C

Private key A encrypts: Encryption "b5...60a3245d2516f7"

Public key A verifies that Private key A was used to encrypt

In an account-based CBDC (left-hand-side), ownership is tied to an identity, and transactions are authorised via identification. In a CBDC based on digital tokens (right-hand-side), claims are honoured based solely on demonstrated knowledge, such as a digital signature.

Source: BIS, Krungsri Research

Account-based CBDCs VS Token-based CBDCs

Identification

Privacy

Security

Transaction Validity

Governance

Transaction Types

Sender Wallet	Receiver Wallet		
	Public User	Business User	Intermediary Nodes
Public User	✔	✔	✔
Business User	✘*	✘	✔
Intermediary Nodes	✔	✘	✔*

Digital Rial Challenges

- Smart Contract Approval Bottlenecks
- No Green Light for Public Blockchain Wrapped Tokens
- Zero Privacy in Small Payments
- Limits on Daily Spending
- No Support for Paying Offline
- Complexities in Blockchain Development