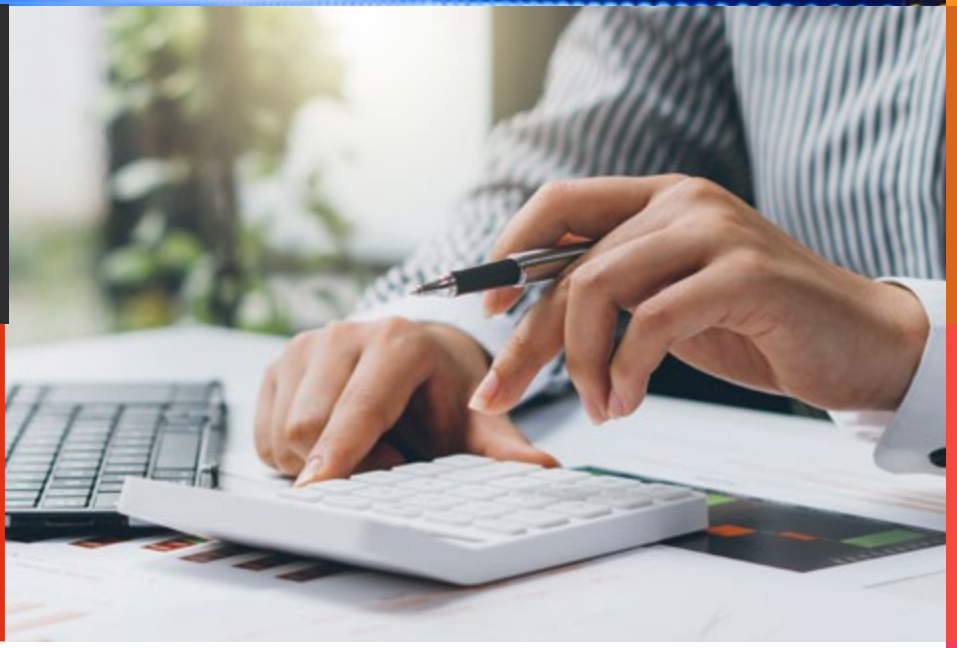
India's digital currency frontier: Envisioning the future of CBDC

November 2024



pwc

Click to launch ▶

Foreword

Dear readers,

It is my pleasure to present the latest edition of our newsletter, which explores the progress of Central Bank Digital Currency (CBDC) initiatives in India.

In this newsletter, we have discussed the growth and journey of CBDC in India with a focus on the pilot and the learnings obtained during these trials. We have then explored the future of CBDC features and technology in India, focusing on key areas such as offline, programmability, wholesale cross-border payments and possible measures to reduce financial fraud using CBDC. Additionally, key technological considerations essential for CBDC implementation are analysed – including privacy, transaction speed, devices and interoperability.

I trust that you will find this newsletter both informative and insightful, offering a clear perspective on the future of digital currency in India and its potential to transform financial transactions and enhance economic efficiency.

For further details or feedback, please write to:

vivek.belgavi@pwc.com or **mihir.gandhi@pwc.com**

Contents

01 Introduction

1.1 About CBDC

Central Bank Digital Currency (CBDC) is denoted as a digital form of fiat currency issued by the central bank, which has the potential to transform the way we transact and engage with money. With CBDC emerging as a payment instrument in the financial landscape, its potential implementation is being actively explored globally. Considering India where digital payments have observed significant growth, CBDC could further accelerate the nation's journey towards a cashless and robust payment framework.

1.2 Basic characteristics of CBDC

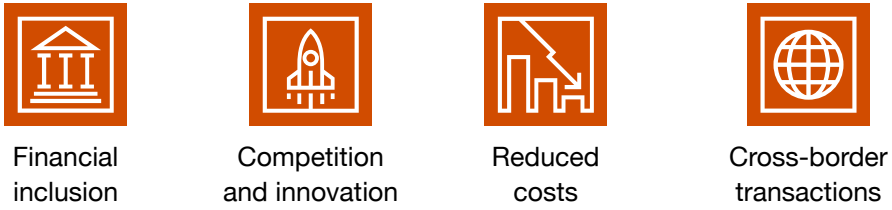
CBDC has already been comprehensively covered in our several publications which could be easily accessed through PwC's CBDC webpage. Some fundamental characteristics of CBDC have been listed below for our new readers:

- **Legal tender:** CBDC is accepted as legal tender which indicates that it is recognised and accepted for transactions within the boundaries of the issuing jurisdiction.
- **Digital money:** CBDC exists only in digital formats. It can be accessed through smartphones and feature phone devices where it can be stored in digital wallets.
- **Different variants:** There are two main types of CBDCs: Retail (accessible by individuals) and wholesale CBDCs (used by financial institutions or banks for large-scale transactions).

1.3 Benefits of CBDC

If we consider CBDC a payment rail, specifically for the Indian context, it offers some key benefits to the stakeholders involved. These benefits are listed below:

Figure 1: Benefits of CBDC



In this newsletter, we look at digital currency and analyse the potential benefits, use cases, challenges and roadmap for the development of CBDCs in India.

02 CBDC pilot: Journey so far

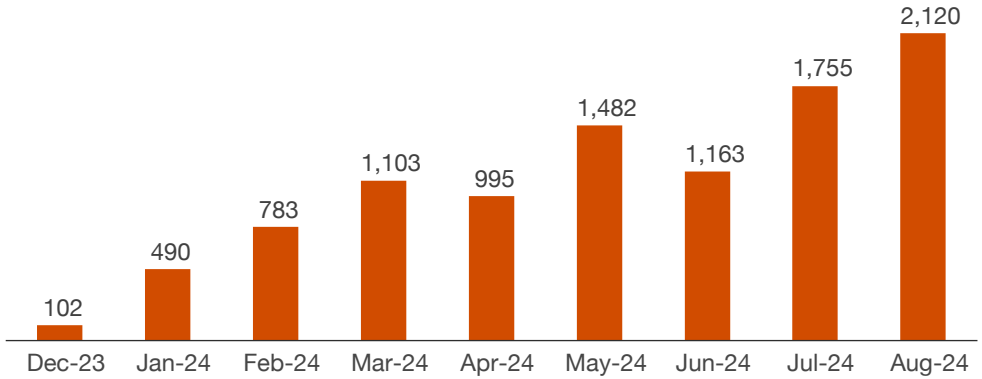
1.1 Background

India kicked off its CBDC journey in 2022 as the Reserve Bank of India (RBI) launched a pilot program with focus on both the retail and wholesale segments. This initiative has been further supported by key financial institutions and FinTech innovators.

Retail CBDC (e₹-R)

The pilot for retail CBDC was launched in December 2022 by the RBI. The program was initially rolled out for peer-to-peer (P2P) and peer-to-merchant (P2M) transactions in select cities but was expanded quickly. As of 13 September 2024, the retail CBDC balance was INR 688.2 crore with a transaction volume of e-RUPI 372.8 lakh with the highest denomination of 500 worth INR 564.29 crore. Till June 2024, the program onboarded approximately 50 lakh consumers and around 4.2 lakh merchants.[1,2] Currently, 13 banks are providing this facility to their customers under the pilot program.[3]

Figure 2: Total value of e-RUPI retail CBDC per month

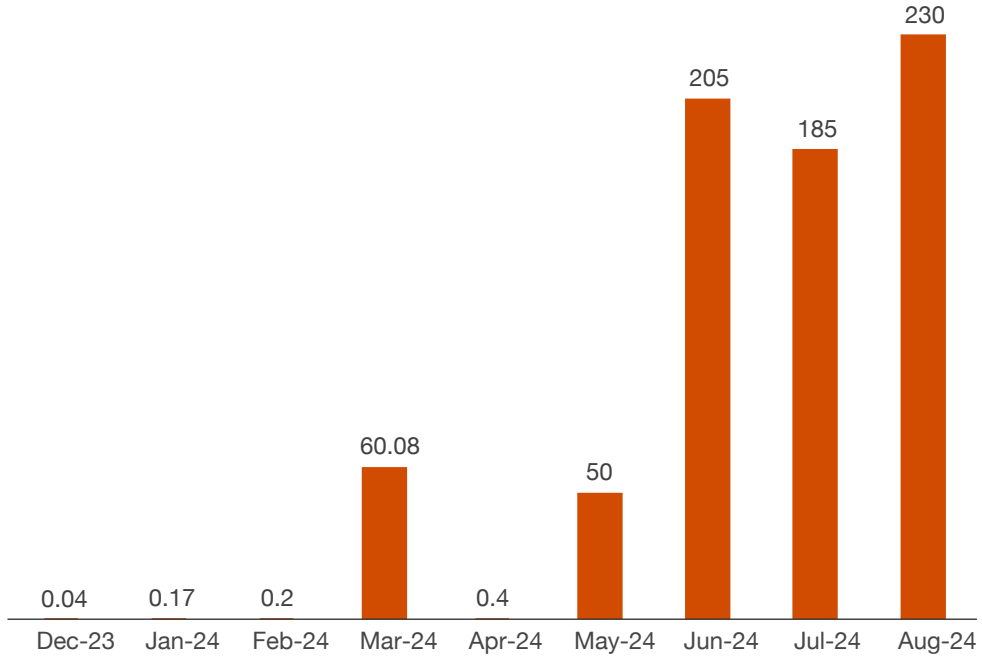


Source: RBI

Wholesale CBDC (e₹-W)

India introduced its wholesale CBDC pilot project in November 2022, primarily focused on settling secondary government bond market transactions. In October 2023, the RBI introduced a new use case for the e₹-W pilot to facilitate settlement of interbank call money trades. This allowed banks to settle these trades in real time using e-Kuber, proving an alternative to interbank RTGS settlements.[4]

Figure 3: Total value of e₹-wholesale per month



Source: RBI

1 https://rbi.org.in/Scripts/BS_CurrencyCirculationDetails.aspx?id=4485
2 https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF
3 https://www.iba.org.in/cbdc/#:~:text=Currently%2C%20the%20pilot%20is%20ongoing,this%20facility%20for%20their%20customers
4 https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT202324_FULLDF549205FA214F62A2441C5320D64A29.PDF

02 CBDC pilot: Journey so far

Expanding use cases for CBDC in India

The RBI has been actively exploring new cases to expand the scope of CBDC pilots:

- Ability to transact offline in situations with poor/limited/restricted internet access such as hilly terrains, internet curfews and cantonment areas
- Exploring programmability in transactions by setting conditions on factors such as location, purpose, user access and time for use cases such as fund distribution to beneficiaries and offering tokenised CBDC rewards
- Leveraging CBDC to offer seamless lending through the Unified Lending Interface (ULI) platform
- CBDC-enabled international payments for use cases such as retail remittances and wholesale interbank settlements

Impact of FinTech enablement in CBDC distribution

Participation of major FinTech companies is key to wider CBDC adoption as RBI continues with its pilot program. Previously, these companies were crucial in boosting user engagement and transaction volumes which ultimately led to the success of the Unified Payments Interface (UPI). Similarly, for CBDC, FinTech companies can roll out the following offerings which could help drive CBDC adoption.

- **Rewarding user loyalty:** FinTech platforms could introduce innovative features to boost the adoption of CBDC. Moreover, platforms with integrated shopping services could offer CBDC cashback and coupons for payments made with CBDCs, providing tangible benefits and enhancing the overall user experience.
- **Gamification strategies:** Gamification can create interactive and rewarding pre- and post-transaction experiences for users. These could include earning points, badges or levels for completing certain transactions, with the potential to unlock more benefits.

2.2 Learnings from the CBDC pilot

The ongoing CBDC pilot has enabled the regulator to improve the offering basis the learnings observed, some of which are:

- **Awareness and adoption:** There is a need to educate the public about the benefits and usage of CBDC to drive adoption. Building trust among consumers about the safety and reliability of CBDC is crucial for its success.
- **Business perspective:** CBDC can streamline financial transactions, reducing the time and cost associated with traditional banking processes. It can offer greater transparency in transactions, which can help reduce fraud and improve trust in business transactions. However, there is an absence of a strong commercial model for Tier-2 stakeholders in the current CBDC offering.
- **Technology perspective:** The pilot highlights the feasibility and challenges of using distributed ledger technology (DLT) for a national digital currency. It is crucial to ensure that the CBDC infrastructure is scalable, efficient, interoperable and secure.
- **Risk perspective:** Ensuring user privacy while maintaining transparency and regulatory compliance is a delicate balance, which needs to be maintained while assessing the potential impact of CBDC on traditional banking systems.

03 What's next for CBDC in India?

New development in the CBDC space with the participation of different entities in the Indian markets and proactive regulatory support shall give rise to various new features. Some key features along with their possible models and use cases are discussed in the following sections.

3.1 Offline transaction models

Digital transactions have proven to be crucial in the development of the payments industry in the country. Offline transaction capabilities provide a reliable alternative during network outages or in areas with poor connectivity. An unstable internet connection could pose a problem in transacting successfully even in urban areas or during internet curfews. During contingencies like natural disasters, or network failures, such a capability could act as a fallback to ensure seamless continuity of transactions and access to essential goods and services.

Limitations in the adoption of offline capabilities

While offline digital payments have been explored as a potential solution to various challenges in India's payments ecosystem, some possible limitations have hindered their widespread adoption, as shown in Figure 4.

Figure 4: Limitations in the adoption of offline capabilities

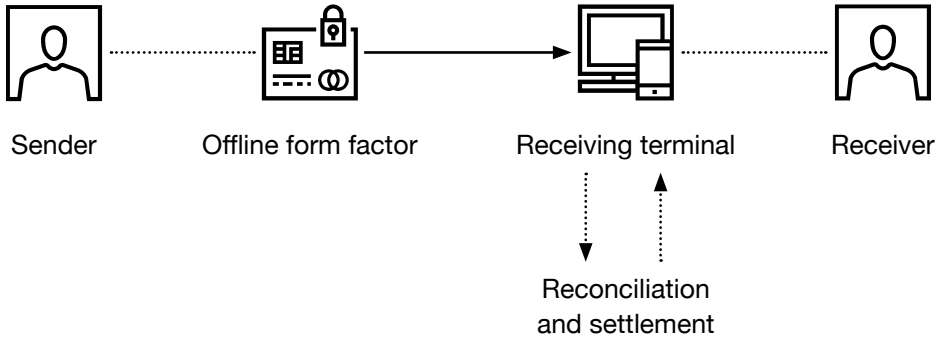
Our viewpoint on possible offline models

While various central banks worldwide are exploring offline capabilities in CBDC, the need to develop a sustainable model is driven by factors such as financial inclusion, protection against cyber frauds and attacks, and business continuity during temporary or prolonged internet disruptions.

Several models can be considered for implementing offline transaction capabilities in CBDCs such as below:

Hardware token-based model

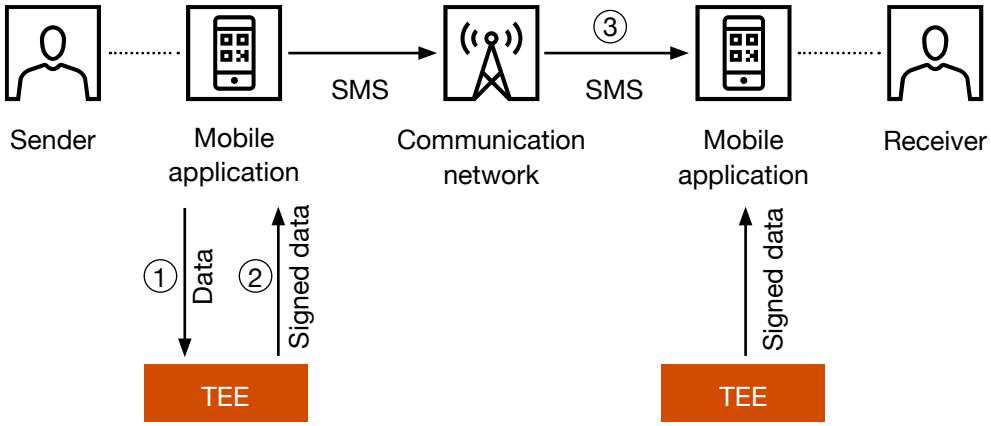
Figure 5: Hardware token-based model



This uses form factors like smart cards, e-SIMs to store and transfer CBDC offline. User transfers CBDC to the hardware token while online, which could be used to perform transactions offline by connecting to other devices or point of sale (POS) systems. This model comprises secure hardware modules and tamper-resistant elements. Transactions are executed while being temporarily offline, yet internet connectivity is required for reconciliation and settlement. However, there is a dependency on physical infrastructure which carries significant costs and is relatively less secure.

Software wallet-based model

Figure 6: Software wallet-based model

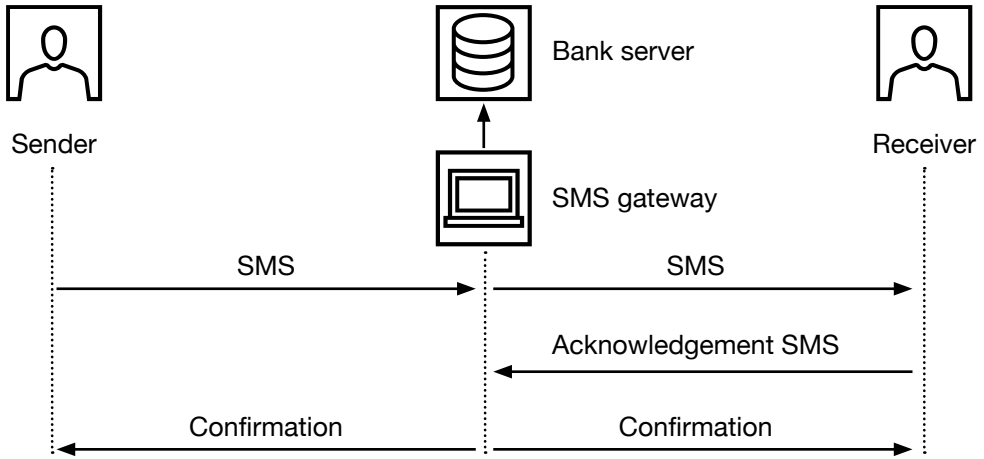


This model uses mobile phones (smartphones or feature phones) equipped with secure elements in the form of trusted execution environments (TEEs). Users download CBDC in the software wallets on mobile phones when online. Additionally, consecutive offline payments are possible in such models. However, they are limited by the condition of availability of a secure element in the payer's device. The highlighting aspect of such software wallet-based models is that they could be used for both proximity as well as non-proximity transactions.

Offline transactions can be conducted using near-field communication (NFC), Bluetooth, telecom or QR codes between devices. Encryption and secure storage within the device protect the CBDC tokens as well as the transaction data.

Hybrid model

Figure 7: Hybrid model



This model combines both approaches using software and hardware to leverage the strengths of each approach for enhanced reliability and user experience. Users may employ a combination of smart cards, mobile wallets and hardware tokens. This model provides perpetual offline transaction capability, integrating multiple layers of security from different technologies to protect user transactions against various threats. The most prominent hybrid model for offline transactions uses telecom for settlement in the absence of reliable internet connections. Hence, this is a secure, low-cost and infrastructure-light model that is interoperable with multiple payment rails.

Each of the models discussed above addresses the limitations in its own way. For example, while CBDC as a payment instrument is more secure than others, these proposed offline models do not become infrastructure-heavy or create the need for huge upfront investments. Additionally, these models are interoperable with the existing payment rails and market infrastructure as well.

Risks in offline transactions

As with any innovative technology, there exist certain risks in implementing the CBDC offline models. We've listed some key risks below with their mitigation strategies:

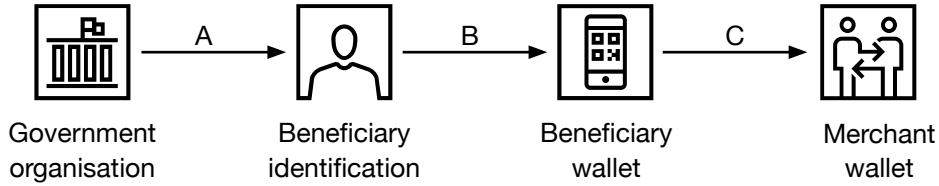
- **Double spend risk:** The double spend risk is where the fund in the offline transaction is spent multiple times while the device is still not connected to the ledger. This can be mitigated by implementing methodologies like controlled offline payment by limiting the value and volume of transactions.
- **Risk of security attack:** Security attacks can be mitigated by the usage of cryptographic protocols and algorithms with appropriate hardware protection.
- **Operational risk:** The risk of the device being lost, or the value being lost in the device, can be mitigated by designing robust governance protocols.

3.2 Programmability enabled with CBDC

Another key facet of CBDC-based transactions is the capability to program the transactions. This ability of embedding smart contracts in transactions along with adding conditions such as geofencing and merchant category code (MCC) enable the programmability of CBDC in India. Through this feature, the programmer can provide better control over the end use of funds. This ensures that payments are only made when certain conditions are met, reducing the need for intermediaries.

Programmability also provides a range of functionalities that traditional money does not offer, leading to more efficient and innovative financial services.

Figure 8: Programmability-based fund distribution to beneficiaries of CBDC



Detailed steps for government-to-person direct benefit transfer

Step A: Fund allocation for beneficiaries identified and verified

Step B: Beneficiary-related condition fulfillment in smart contract for CBDC deposit by Government

Step C: CBDC redemption at authorised merchant outlet as per smart contract conditions

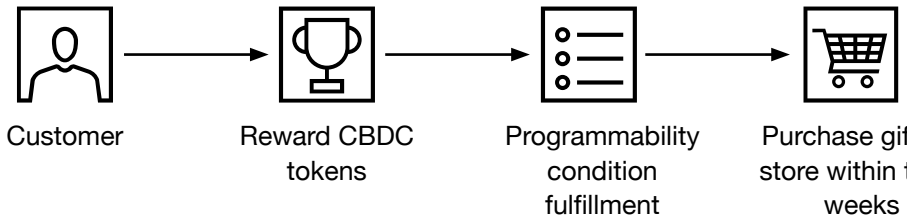
03 What's next for CBDC in India?

While direct benefit transfer (DBT) has been considered a strong proposition by the Government for extending subsidies to the beneficiaries using the programmability feature in CBDC, Subhadra scheme for Odisha might become the first one to use CBDCs, benefitting more than 1 crore women in Odisha.[5]

Case study: CBDC token as rewards in a loyalty program

A financial institution is launching a loyalty program for its customers and merchants. The rewards here are in the form of CBDC tokens, programmed to be used at designated merchant points only. Here, the financial institution has set spending conditions like geographical location, spending amount, expiration date and merchant category, to name a few. To make such an arrangement financially viable, incentives for the financial institution in the form of commissions from the onboarding merchants could be charged as well. A leading public bank in India has recently introduced such a loyalty program for merchants.

Figure 9: CBDC token as rewards in a loyalty program



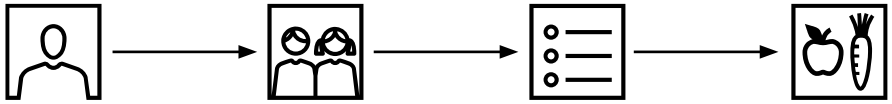
For example, a customer redeems the earned rewards of such a loyalty program, and their CBDC token is programmed to be used for purchasing gift items (purpose) at a physical store of the shopping platform (geofencing) within three weeks of redemption (period). So, a customer's redemption will only be successful after he/she fulfils these conditions. At the merchant's end, these are normal CBDC tokens that can be used in consecutive payments.

5 https://www.pmindia.gov.in/en/news_updates/pm-launches-subhadra-the-largest-women-centric-scheme-in-bhubaneswar-odisha/?comment=disable

Case study: User-level programmability

A financial institution could consider enabling user-level programmability using CBDC tokens. In such a scenario, users get the flexibility to set controls over the spending of the CBDC tokens. Spending conditions can be controlled through geographical locations or merchant categories. A leading private bank in India has recently launched user-level programmability for its customers using CBDC.

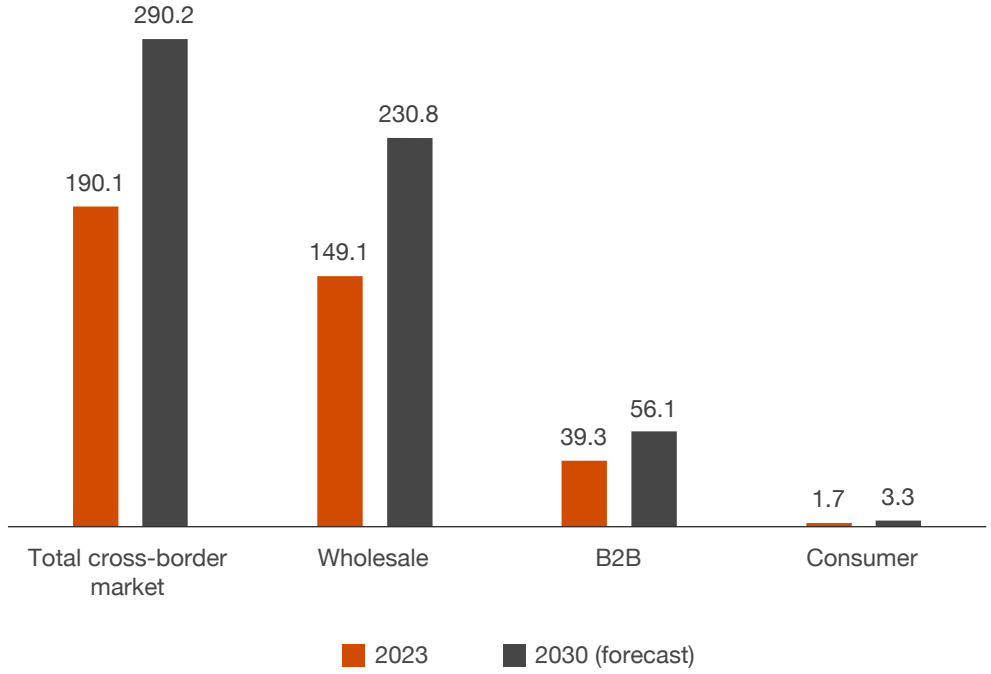
Figure 10: User level programmability



For example, a parent holding CBDC tokens may give monthly pocket money to the child. To exercise control on spending, the parent may decide that tokens can only be spent within the school premises (geofencing) to purchase snacks (purpose) from the canteen for a particular month (period). Transactions will only be successful on fulfilment of these pre-specified conditions.

3.3 Wholesale cross border

Figure 11: Value of cross-border payments (in USD trillion)



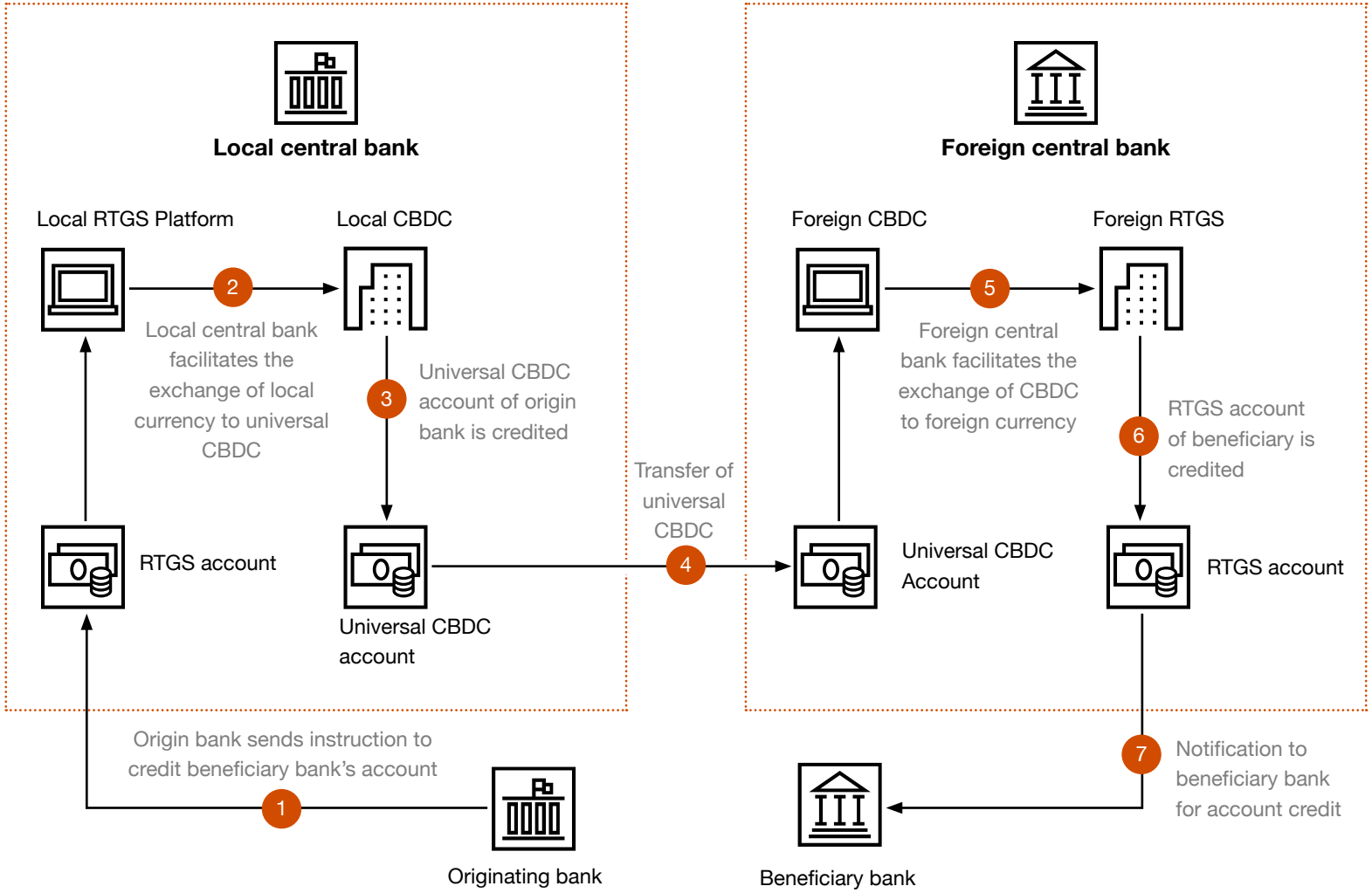
Source: Statista

Market sizing and trends

There has been a visible surge in international trade, foreign investments and e-commerce-led consumerism over the last decade, courtesy of globalisation and digitalisation. This increase in the flow of money across borders can be accounted for in terms of the sheer value of worldwide international payments which stands at more than USD 190.1 trillion.[6]

The wholesale segment of cross-border payments involves transactions that occur between banks, investors and hedge funds. The major chunk of this segment is contributed by the foreign exchange market (FX) which is responsible for determining the exchange rate for every currency. Outside of the wholesale segment, remittance flows to low- and middle-income countries (LMICs) are a major constituent of consumer-initiated cross-border payments and are expected to grow rapidly owing to the ever-increasing international migration.

Figure 12: Extending local CBDC to a universal token model for cross-border payments



6 https://www.pmindia.gov.in/en/news_updates/pm-launches-subhadra-the-largest-women-centric-scheme-in-bhubaneswar-odisha/?comment=disable

03 What's next for CBDC in India?

Figure 13: Wholesale cross-border CBDC market sizing and trends

USD **7.5** trillion
Average daily trade volume in FX market

1.6%
Average daily turnover of INR in FX

USD **669** billion
Remittance flow to LMICs in 2023

USD **125** billion
Remittance inflow in India in 2023

6.35%
Annual costs of sending remittances

Sources: BIS; https://www.worldbank.org/en/news/press-release/2023/12/18/remittance-flows-grow-2023-slower-pace-migration-development-brief; https://data.worldbank.org/indicator/BX.TRF.PWKR.CD.DT?locations=IN; https://remittanceprices.worldbank.org/

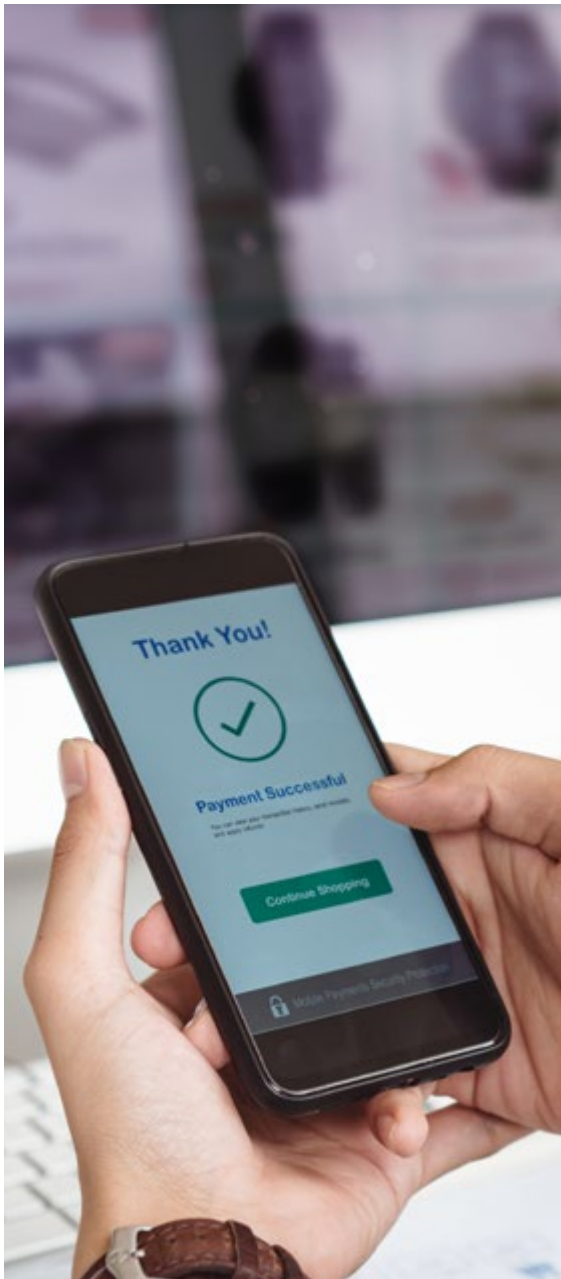
Potential use for wholesale CBDCs in cross-border payments

CBDCs have the potential to improve the efficiency and risk management of the settlement process in the cross-border space. The working model for extending local CBDC to a universal token model for cross-border payments across use cases will be beneficial in a much more streamlined manner (Figure 12). The idea presented in this model – connecting the domestic instant payment systems to a universal CBDC network – is the focal point of Project Nexus.[7] This is an initiative by the Bank of International Settlements (BIS) and has India as one of the participating nations.

Replacement of traditional nostro-vostro framework in institutional payments ecosystem

The current state of the correspondent banking system involves multiple intermediates that operate at different working hours. In a scenario where the nostro account of a client is not topped up enough for an onward payment, the correspondent sometimes credits the client to make a payment. These credits can be intraday or even longer. This creates an uncertain environment of trapped balances in nostro/vostro accounts.

- CBDCs can help solve this problem statement wherein each central bank maintains an on-chain nostro account on the corridor network for efficient interbank transfers.
- Project Dunbar and mCBDC Banque de France-MASJP Morgan ONYX[9] are key projects experimenting along the same lines.



7 https://www.bis.org/publ/othp86.pdf
8 https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm
9 https://www.banque-france.fr/en/press-release/banque-de-france-and-monetary-authority-singapore-break-new-ground-cbdc-experimentation

Atomic settlements of payments

The current system of international payments is slow and expensive. Atomic settlements involve a simultaneous exchange of two assets (payment and delivery) that takes place when certain conditions are met.

- CBDC-enabled hashed-timelock contracts (HTLC) can provide a safe blockchain-based settlement model.
- A Singaporean startup has recently developed a product to facilitate the atomic settlement of transactions using blockchain technology and smart contracts.[10]

Liquidity pools

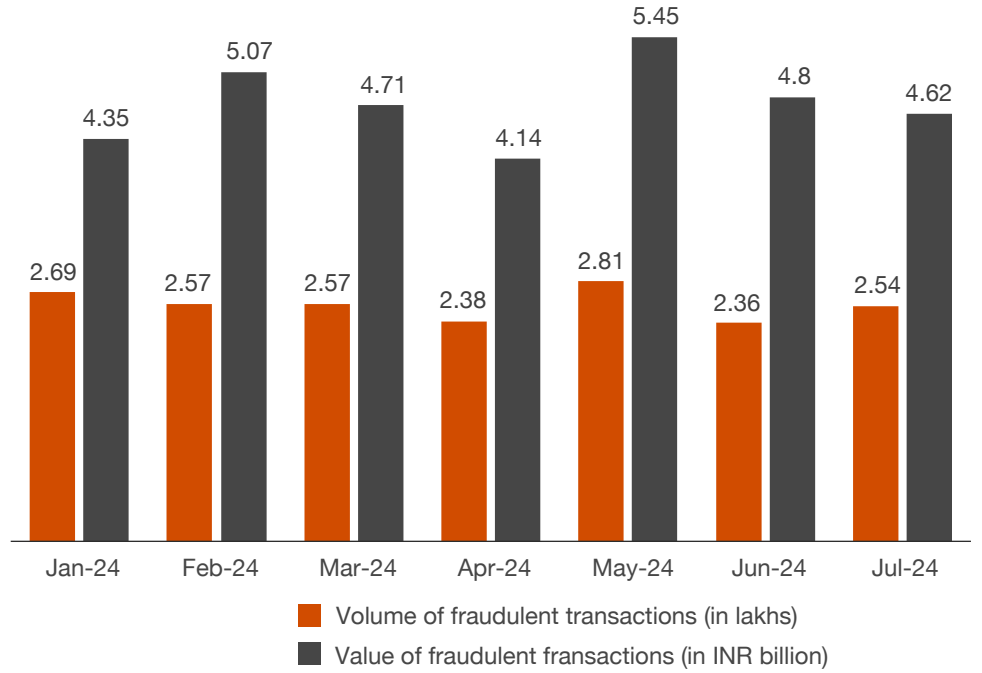
The correspondent banking system characterised by long settlement hours locks up the much-needed working capital causing liquidity-related issues for financial institutions.

- CBDCs can make use of automated market markers (AMMs) to counter this challenge by providing liquidity provisions for illiquid assets by pooling assets to determine asset prices in the FX market.[11]
- They operate 24x7 due to their automated decentralised exchange protocol and offer instant on-chain settlements.
- The concept of AMMs in non-crypto settings is currently being explored by BIS in projects such as Project Mariana.[12]

3.4 Zero financial fraud using CBDC

Financial fraud is a major concern in the Indian payments landscape with the ever-increasing volume of cashless transactions. As of July 2024, India witnessed a fraudulent transaction for every 71,157th domestic financial transfer.[13] Wider adoption of CBDC can help counter this challenge by offering a solution to mitigate fraud, owing to its traceability and transparency.

Figure 14: Domestic payment fraud in India



Source: RBI

10 https://www.forbes.com/sites/zennonkapron/2022/12/21/the-future-of-cross-border-payments-in-asia-is-atomic/
11 https://www.imf.org/en/Publications/fintech-notes/Issues/2024/05/15/Cross-Border-Payments-with-Retail-Central-Bank-Digital-Currencies-547195
12 https://www.banque-france.fr/system/files/2023-09/20230928%20Mariana%20final%20report.pdf
13 https://rbidocs.rbi.org.in/rdocs/PSI/PDFs/PSIJULY2024355A835657974FF0A2E080BEBE5C3C41.PDF

03 What's next for CBDC in India?

The RBI Act amendment[14] views CBDC and paper currency with the same lens, and henceforth, the parameters enforced by the income tax department for cash payments and withdrawals apply to CBDCs as well.[15] Therefore, the identity of a CBDC user may be established on a need basis by the authorities, when the user draws funds from banks to place in his/her CBDC wallet, owing to banks' KYC norms. Each CBDC token is characterised by a unique and immutable identifier. This makes it possible for the anti-money laundering/countering the financing of terrorism (AML/CFT) authorities to trace the entire wallet-to-wallet trail for a token from its point of origin, in case of frauds such as siphoning and tax evasions.

In cases involving agreement-based payments, the programmable nature of CBDCs can be leveraged to time-lock a transaction for a certain period, which would then require credentials from all concerned parties in order to get executed. If the transaction is not executed within the given timeframe, the funds are reversed to the original owner, thus preventing fraud and facilitating a smooth process for payment-related dispute resolution.

Case study: Countering money mule accounts

Money muling is a type of financial fraud wherein a fraudster uses a third person's account to move money illegally. The following features offered by CBDCs can help counter such cases related to money mule accounts:

- **Trackability and traceability:** Compared to cash or other forms of digital currency, CBDC transactions can be tracked and traced back since they are recorded on the central bank's ledger. Thus, this helps in identifying the fraud chain of money mule accounts.
- **AML measures:** Integration of CBDC systems with robust AML measures would help in real-time transaction monitoring, identification of suspicious activities and immediate action against frauds.
- **Programmability:** Implementing strict controls and regulating the volume and value of transactions, courtesy the programmable nature of CBDCs, would help in preventing frauds.

Case study: Strengthening CBDC networks

In November 2023, the BIS Innovation Hub Swiss Centre developed a Project Tourbillon[16] which proposes a lattice-based blind signature scheme as a replacement to the current asymmetric cryptography techniques such as RSA-based encryption, Diffie-Hellman key exchange and digital signatures. This was aimed at protecting CBDC networks from cyberattacks and large-scale financial frauds.

The European System of Central Banks (ESCB)'s EUROchain research network has proposed the use of a DLT platform, Corda, to ensure compliance with AML/CFT regulations and ensure user privacy and cyber safety in CBDC networks.[17]

- The platform provides a privacy solution such that the user's identity and transaction history cannot be accessed by intermediaries or entities – except for the entities chosen by the user.
- Additionally, users are given pseudonymous identities which act as network addresses for CBDC payments.
- Further considerations for the project include using mechanisms such as rotating public keys and enclave computing.

The findings from these projects could be leveraged in creating a model to reduce financial fraud in India. While the focus remains on mitigating fraud, this should be done whilst ensuring that the core principles of a CBDC – user privacy and token anonymity – remain intact. The strengthening of encryption protocols and transaction surveillance mechanisms must be incorporated by financial institutions (and private payment service providers in the future) for fraud prevention. This must be built by leveraging zero-knowledge proofs to ensure data minimisation and user privacy. Additionally, the concept of reversibility could be explored in CBDCs so that fraudulent transactions can be reversed back to the victims.

14 https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf
15 https://www.financialexpress.com/business/blockchain-explainer-can-the-cbdc-be-anonymous-2907000/
16 https://www.bis.org/publ/othp80.pdf
17 https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

04 Technology considerations for CBDC

While various use cases of CBDC develop as per the requirements of the users, the infrastructure requires certain technological considerations as well, which are highlighted below.

4.1 Privacy enhancing technologies

The amount of visibility into the transactions for different stakeholders such as mobile wallet infrastructure providers and banks should be carefully considered. Additionally, support for zero - knowledge proofs, homomorphic encryptions and ring signatures could be considered to protect the privacy of CBDC users.

4.2 Transaction speed considerations

Having seen the issue of low ticket size with UPI, it is essential to set realistic expectations for key metrics such as uptime, transaction throughput and transaction speed – especially for payment and settlement of low-value and high-volume transactions.

4.3 CBDC API

The regulator could consider implementing an additional API layer in the existing two-tiered structure for supporting offline payments, escrow functionality and verifiable proof of balance without having dependencies on technology service providers (TSPs).

4.4 Devices

The devices (smartphones, feature phones, smart cards, etc.) could include logic and security mechanisms to prevent double-spending and counterfeiting of CBDC tokens. Additionally, these devices should support merchant as well as peer-to-peer payments.

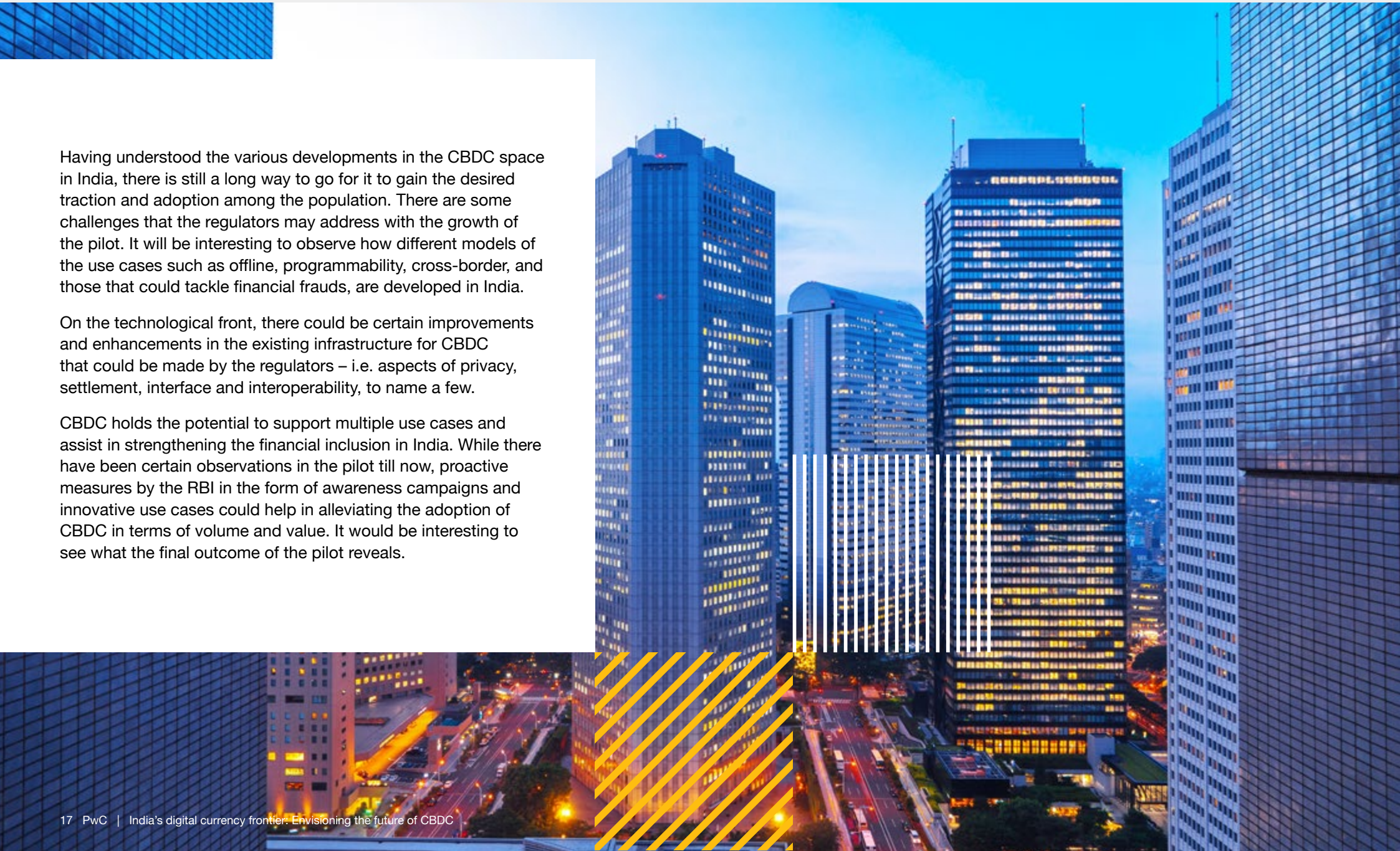
4.5 Interoperability

The regulators need to consider the interoperability of CBDC with cash, domestic payment rails and other international payment rails to enable a holistic ecosystem. Whether the existing infrastructure is capable, or it would require additional infrastructure, needs to be assessed. Simultaneously, interoperability with CBDC mechanisms of nations having significant trade with India should be taken into consideration.

4.6 Identity management

Lastly, the implementation of CBDC wallets with standardised AML/KYC processes considering mitigation of non-uniform identity verification process by individual payment service providers is crucial.

05 Conclusion



Having understood the various developments in the CBDC space in India, there is still a long way to go for it to gain the desired traction and adoption among the population. There are some challenges that the regulators may address with the growth of the pilot. It will be interesting to observe how different models of the use cases such as offline, programmability, cross-border, and those that could tackle financial frauds, are developed in India.

On the technological front, there could be certain improvements and enhancements in the existing infrastructure for CBDC that could be made by the regulators – i.e. aspects of privacy, settlement, interface and interoperability, to name a few.

CBDC holds the potential to support multiple use cases and assist in strengthening the financial inclusion in India. While there have been certain observations in the pilot till now, proactive measures by the RBI in the form of awareness campaigns and innovative use cases could help in alleviating the adoption of CBDC in terms of volume and value. It would be interesting to see what the final outcome of the pilot reveals.

Contact us

Mihir Gandhi
Partner and Leader – Payments Transformation and FinTech
mihir.gandhi@pwc.com

Geetika Raheja
Partner – Payments Transformation
geetika.raheja@pwc.com

Rajesh Dhuddu
Partner – Emerging Technology
rajesh.dhuddu@pwc.com

Zubin Tafti
Executive Director – Payments Transformation
zubin.tafti@pwc.com

Authors:

Pramod Mishra, Kanishk Sarkar, Pushkar Pradhan, Karan Mahajan, Rahul Chemburkar, Aayushya Mudgal, Utkarsh Tiwari and Parth Goyal

Editor:

Rashi Gupta

Design:

Harshpal Singh

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

pwc.in

Data Classification: DC0 (Public)

HS/November 2024 - M&C 42217