Offline transactions using CBDCs

Central banks all over the world are experimenting with a new form of digital currency (e-currency) called central bank digital currencies (CBDCs). These digital currencies will be backed by central banks and will have the same element of safety and trust as physical currencies. While any discussion on CBDCs always revolves around blockchains (online and real-time), it would be a good idea to mimic the characteristics of paper currency, which doesn't require an online medium and can be transferred between people while maintaining complete anonymity.

Paper currency is fungible as each note of a similar denomination is of the same value, yet every note has a unique serial number (token). So each note or coin gets minted and distributed by central banks in a controlled manner. Thereafter, the money gets pumped into the economy with complete anonymity. Taking this idea further, e-currencies can also be minted in a blockchain in a controlled manner and then distributed in an offline mode.

Costs involved for physical currency notes

Printing and raw material costs

Technologies used to maintain the uniqueness of currency notes and coins

Transportation and security costs

Operational costs in the banking system and related technologies like Unified Payments Interface (UPI)

The above costs can be eliminated by switching to an e-currency. Such a currency is also ESG friendly and aligned with net zero initiatives as it would reduce the usage of paper, various dyes as well as CO_2 emissions associated with the transportation of physical currencies.

pwc

Advantages of a CBDC[1]

1 Reduces operational costs involved in physical cash management.

2 Fosters financial inclusion.

3 Builds resilience, since unlike UPI payments, CBDCs can be transacted even if the bank's payment gateways are down.

4 Leads to innovation in the payments system.

5 Makes the payment settlement system more efficient.

6 Boosts innovation in the cross-border payments space.

7 Provides the public with the benefits of private virtual currencies, without the associated risks.

How CBDCs differ from UPI

UPI is an online system for transferring money between banks. A CBDC, on the other hand, follows the peer-to-peer (P2P) model and can be used to transact in an offline mode without involving any bank. Thus, it eliminates the bank as an intermediary, leading to considerable operational cost savings.

Features and characteristics of e-currencies

Every e-currency note would have a non-fungible ERC-721 token – i.e. a unique identity and a value. For example, an INR 20 token will have a digital token ID and would be attributed a value of INR 20. Every time an e-currency is transferred to a purchaser, the token gets burned or destroyed, which means that the role of blockchain ends whenever the token gets transferred as an encrypted file to the purchaser. Subsequently, all transactions happen in offline mode with complete anonymity.

1. Transferrable
2. Programmable
3. Encrypted file formats
4. Cannot be replicated by owners

Prerequisites for CBDCs

1. A government-enabled private Ethereum blockchain, with multiple nodes
2. Camera and Wi-Fi enabled smartphones (for citizens to perform offline transactions)
3. Unique wallets for every citizen
4. Mobile app published by the central bank to transfer e-currencies

Physical vs digital minting

Based on economic needs, central banks will mint a fixed proportion of physical and e-currencies – for instance, 70:30. A centralised blockchain-based application would be used by central banks to mint ERC-721 tokens of various denominations (e.g. 1,000, 500, 200, 100, 50, 20, 10 and coins of 1, 2 and 5).

---

1 https://static.pib.gov.in/WriteReadData/specificdocs/documents/2022/dec/doc2022121139201.pdf

Uniqueness of wallet and e-KYC

The central bank will issue blockchain-based unique wallet IDs for citizens based on citizen identification numbers (e.g. SSN in the US and Aadhaar in India). Each wallet will be also associated with a mobile phone number, which would be used for OTP confirmations at the time of e-currency transfers.

This wallet ID would be mapped with the central bank's mobile application. A unique QR code will be associated with the public key of each wallet.

Proposed solution

1. Procurement of e-currency:

The purchaser of the e-currency will have the following options to transfer it to their wallet:

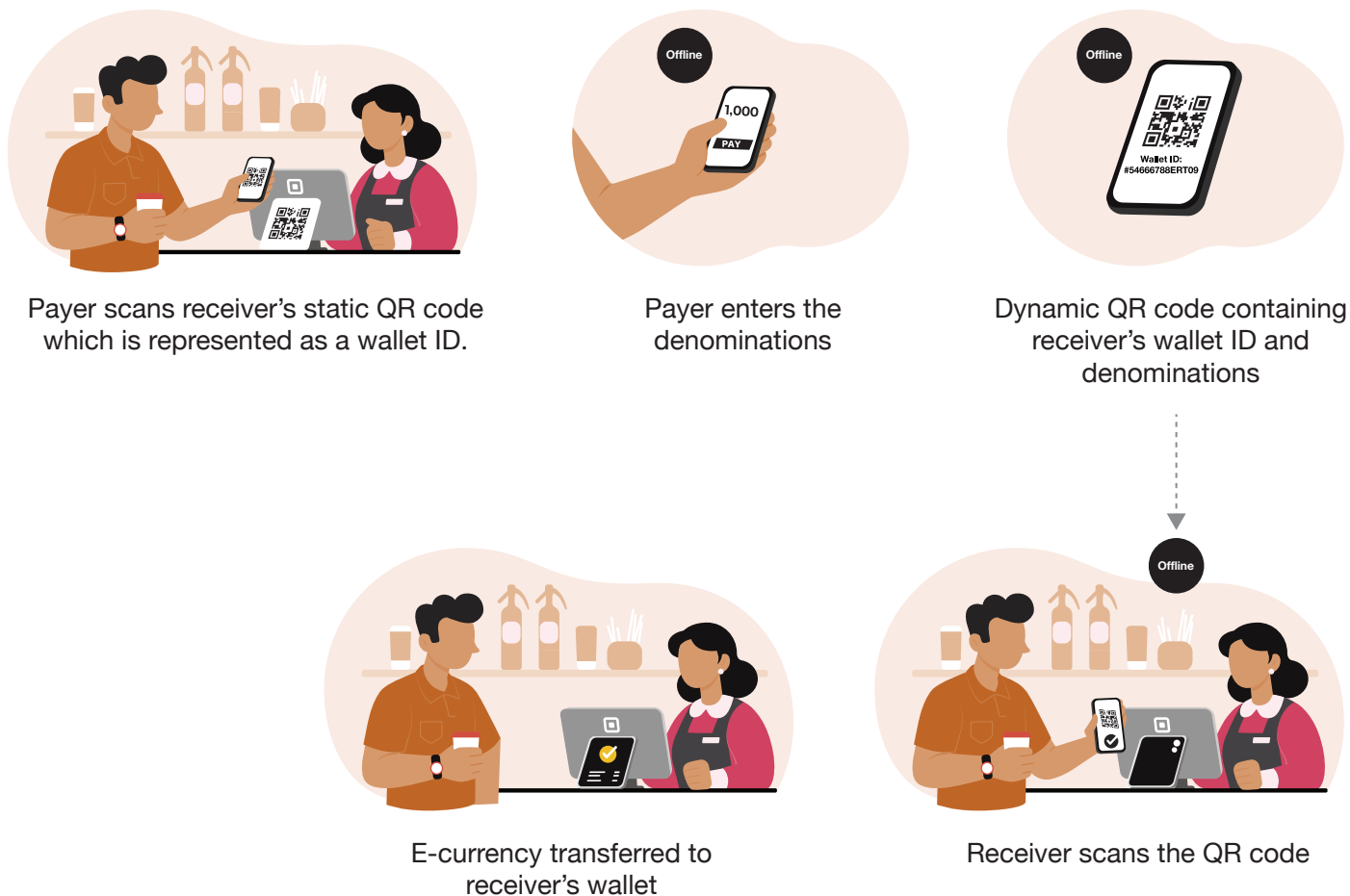|		
Online: Digital payment and transfer of e-currency to their wallet	**Online:** Over counters/ subsidiaries enabled by the central bank, by making physical currency payments and getting the e-currency transferred to their wallet	Each denomination of the e-currency would be stored as a record in an encrypted local database.

2. E-currency offline transactions:

The owner of the e-currency will have the right to make purchases through offline transactions. The e-currency will be transferred by moving the e-currency records between the buyer and seller.

QR code–based offline transaction

Payer scans receiver's static QR code which is represented as a wallet ID.

Payer enters the denominations

Dynamic QR code containing receiver's wallet ID and denominations

E-currency transferred to receiver's wallet

Receiver scans the QR code

How money is transferred

a. The unique wallet QR code would be used for e-currency transactions between two smartphones.

b. The purchaser needs to scan the wallet QR code of the seller and enter the amount to be transferred in their mobile app.

c. The purchaser need to select the e-currency files of various denominations in their wallet that add up to the total amount and generate a unique QR code which will contain (i) the seller's wallet ID and (ii) details of token IDs of all the e-currencies. The e-currency tokens are then deleted from the purchaser's mobile phone.

d. The seller now needs to scan the unique QR code generated by the purchaser through her or his mobile app, following which the e-currency tokens will be added to the seller's local encrypted database.
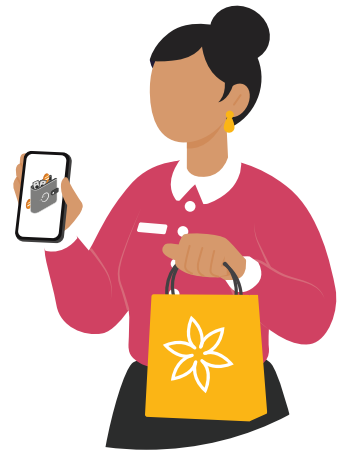
Minting and disbursal of e-currency
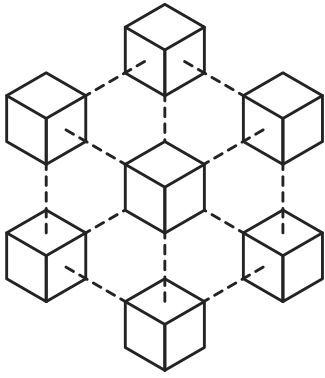
Permissioned blockchain

Central bank mints and disburses e-currency

Loading wallet with e-currency

Programmability of e-currency

Imagine a situation where the central bank has the option to mint some currencies for a specific purpose. For example, in the field of agriculture, education, healthcare, etc., the government could transfer these specially minted e-currencies to the wallets of designated citizens, which could be used for buying fertilisers, paying school/college fees, purchasing medicines, etc.

The programmability feature of e-currencies is suited to these kinds of situations. The government can either mint these e-currencies as 'one-time-use-only' currencies or could re-program them to normal e-currencies upon their use for the designated purpose.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 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.

© 2023 PwC. All rights reserved.

Contact us

Ashootosh Chand
Partner, Digital and Emerging Technologies
PwC India
ashootosh.chand@pwc.com

Indrojeet Bhattacharya
Managing Director, Digital and Emerging Technologies – Web 3.0
PwC India
indrojeet.bhattacharya@pwc.com

Zubin Tafti
Managing Director, Tech Consulting - Payments Transformation
PwC India
zubin.tafti@pwc.com

Contributors

Indrojeet Bhattacharya
Priyabrata Mukherjee
Pooja Jalilkop
Biswanath Das
Zubin Tafti

pwc.in