Central bank digital currency (part 1): Objectives and architectural considerations

2021

Table of contents

Introduction

Central banks worldwide are investigating the potential of central bank digital currency (CBDC) to support them in their mission of ensuring financial and monetary stability.

This paper synthesizes industry research on the topic (see references 1-6), looking at technical implementation approaches based on central bank missions, requirements, and goals.[1]

We start by looking at potential objectives for implementing a CBDC and how those objectives inform design. Then, we propose a set of architectural principles for potential solutions. Our aim is to facilitate discussion in this evolving area and highlight opportunities for further consideration.

For a more technical perspective, read "CBDC (part 2): Technology options and performance criteria," which provides a reference architecture designed to optimally store and process CBDC data, and technical details into how the reference architecture processes and settles transactions (along with specific implementation benefits).

Read now

CBDC objectives

To a large extent, CBDC solution design, architecture, and technology depend on the central bank's goals. Let's look at five primary objectives and the design implications for each.

Objective #1: Improving payment system resilience and competition

Financial stability is a core part of every central bank's mission. CBDC can support a resilient payments infrastructure by establishing a digital alternative that reduces over-reliance on a small number of payment providers.

Current payments infrastructures vary considerably from country to country. In some cases, a small number of providers dominate, like in many parts of Latin America, where credit card fees amount to over one percent of GDP.[2] CBDC can help drive down payment costs and mitigate economic risks of provider service interruption. It can also open up the market to emerging competitors and encourage innovation.

To satisfy this objective, the CBDC solution needs to meet key technical performance criteria, such as high availability and low operating costs.

Objective #2: Increasing financial inclusion

Although physical cash remains popular in many countries, its use as a means of payment rather than purely as a store of value is falling globally. In Sweden, for instance, the number of people using cash fell 32 percent between 2014 and 2018.[3] This trend has also accelerated during the COVID-19 pandemic.

This is a particular concern for emerging economies without high quality electronic commercial banking mechanisms and/or payment systems.[4] In many countries, a large proportion of the population lacks access to a bank account, meaning physical cash is their only payment option. A CBDC system, implemented together with other national initiatives such as identity management schemes could expand financial inclusion by replicating some benefits of physical cash, such as ease of use and the ability to carry out transactions offline.

Cambodia is currently piloting the Bakong CBDC system.[5] By combining CBDC with a national identity management initiative, it aims to be a catalyst for broadening access to financial services within underbanked communities.

Objective #3: Meeting future payment needs in an increasingly digital economy

One of CBDC's greatest potential benefits is the ability to build functionality into a currency. That way, it can serve as programmable money and support micropayments.

Some distributed ledger technologies (DLTs), such as the blockchain platform Ethereum, are designed so that a central bank can apply automated transaction conditions and logic to a CBDC solution. Technology experts sometimes refer to these transactions as being based on smart contracts because they are subject to the execution of code. The effect can be similar to an escrow arrangement but automated. Once relevant conditions are satisfied (such as delivery of goods or services), the system executes the transaction without further human intervention, making it programmable money.

There are many potential use cases for programmable money. It can enable an Internet of Things (IoT) model, where Internet-connected sensors and microcomputers monitor provision and receipt of microservices as they happen. And it can support very small transfers, known as micropayments.

Programmable transaction systems operate today. For example, Singapore Exchange Limited (SGX) uses Amazon Managed Blockchain to allow buyers to trade digital cash for government bonds—without intermediaries and with increased transparency and security.[6]

Find out more

Programmable money is often associated with tokens and blockchain, but other approaches provide the same or similar functionality. For example, Amazon Quantum Ledger Database (Amazon QLDB) is a fully managed ledger database service that you can use with smart contract tools. Commercial sector payment services providers (PSPs) can also offer programmable money powered by a core ledger as an overlay service. Application programming interfaces (API) can then link different PSPs operating a smart contracts solution.

AWS believes central banks have an important role setting smart contract standards to ensure interoperability between and with PSPs. Standards should be set nationally for smart contracts operating domestically and internationally for cross-border transactions.

Objective #4: Improving cross-border payments

In October 2020,[7] the Financial Stability Board defined ways to improve cross-border payments. Its recommendations included updating existing methods, adopting new international standards, introducing new platforms for cross-border payments, and potentially using CBDC systems for cross-border payments. The report left open the possibility for central banks to use either wholesale or general purpose CBDCs as the basis for a solution.

Wholesale CBDCs

In some respects, the concept of a wholesale CBDC is similar to the idea of expanding availability of central bank reserve accounts beyond established commercial banks. Financial services institutions in the commercial sector are already using this approach for cross-border payment innovation.

In 2018, the Bank of England granted TransferWise, a fintech specializing in cross-border payments, access to a central bank reserve account. This enabled TransferWise to settle transactions more easily, which resulted in annual cost savings of £1 billion across its six million consumer and business customers.[8] A wholesale CBDC could facilitate these sorts of benefits at a much wider scale.

Find out more

General purpose CBDCs

There's another possible approach if cross-border payments involve two countries that both operate general purpose CBDCs (also referred to as retail CBDCs). Transferors could initiate transactions through a commercial bank or PSP. It would then go through a clearing process with the PSP acting on the other party's behalf. The first national CBDC system would cancel the currency after transferring it, and the receiving country's CBDC system would generate new currency of equivalent value. The parties would have to agree on an exchange rate or base it on an index.

This approach depends on cooperation between central banks and interoperability between CBDC solutions. Interoperability would depend on a number of agreed-upon standards and processes, which an internationally recognized entity would have to manage. For example, even if ISO 20022 applied to CBDC solutions, there would still be questions about APIs and implementation for different payment types. Interoperability would also rely on new supporting infrastructure, such as international networks for clearing between PSPs and settling between central banks.

Benefits of interoperable general purpose CBDC systems

- **Simpler, faster transaction flows**
  Only relevant parties' PSPs are involved and no intermediary correspondent banks are required for settlement. Settlements could happen in seconds, depending only on CBDC system processing speeds.

- **Enhanced security**
  They enable additional oversight for applying sanctions, detecting fraud and money laundering, and monitoring suspicious activity. This additional oversight layer could involve analyzing data passing through a centralized settlement system, similar to an approach for preventing unlawful domestic activity.

Objective #5: Preventing unlawful activity

Another key CBDC design requirement is tracking mechanisms to detect unlawful activity like money laundering, fraud, and sanction violations. This isn't currently possible in a traditional cash-based system.

Ability to detect unlawful activity at different stages with CBDC data

- **Monitoring individual CBDC transactions**
  Fraud detection and sanction checks can be conducted in real time (similar to what SWIFT offers for cross-border transactions[24]) using machine learning techniques to gain insight from CBDC transaction data.
- **Analyzing and detecting patterns across CBDC transactions over time**
  These insights can help government agencies and PSPs discover money laundering activities, and quickly identify and freeze transactions/accounts participating in suspicious activity. Agencies can also enable solutions powered by artificial intelligence and machine learning to improve detection accuracy.

One key consideration for central banks: How do you deal with CBDC's potential to replicate the anonymity of physical cash? This feature can be key to financial inclusion, but there are implications for managing risk and detecting unlawful activity.

Regulators can control privacy and anonymity levels at different layers of a CBDC architecture.[25] For example, they could design it so no party identity information passes between transaction participants. This would mirror some anonymity characteristics of physical cash.

The same CBDC solution would still require identity verification as part of anti-money laundering (AML) checks when people open a CBDC account. PSPs facilitating transactions could then record participant identities. This would allow law enforcement to trace transactions if they suspect criminal activity. A solution like this isn't truly anonymous, but it does provide a degree of user privacy. The central bank of Cambodia adopted this mechanism for its CBDC pilot.[26]

Architectural considerations

Given these five objectives, what are architectural considerations and best practices for a CBDC solution?

Let's look at six primary categories. We'll focus on general purpose CBDCs designed for all market participants rather than wholesale CBDCs, which only specific PSPs such as commercial banks can use.

Direct versus two-tier architectures

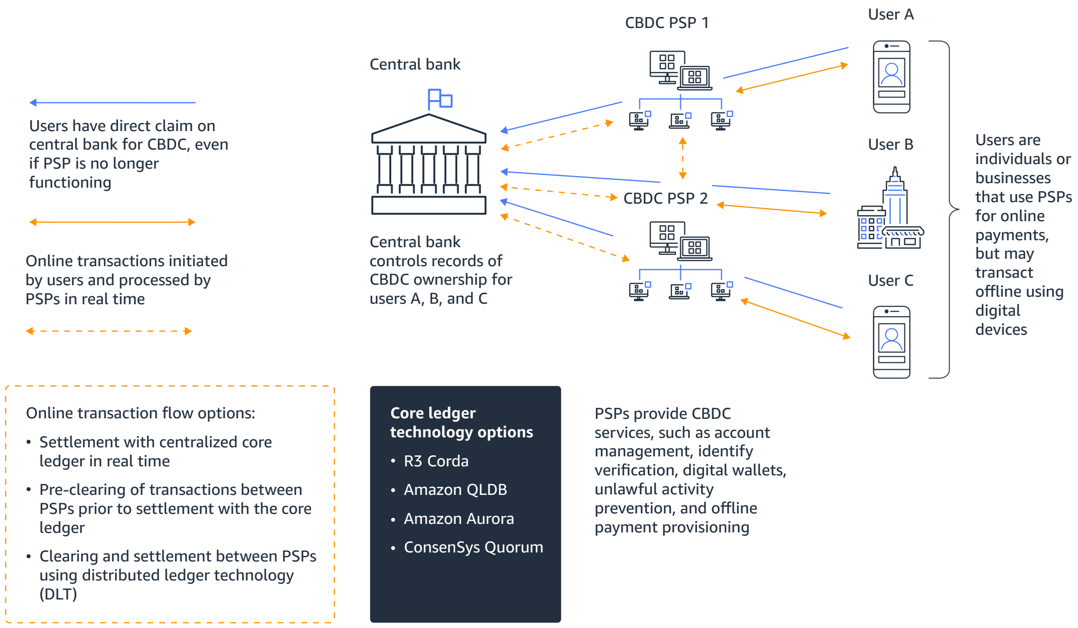
There are two broad architectural options to support a general purpose CBDC:

- A direct architecture allows transactions to take place through a direct connection between individual CBDC users and the central bank (or a central services provider acting on the central bank's behalf).
- A two-tier architecture involves CBDC users interacting with each other through PSPs (such as commercial banks).

The two-tier architecture allows central banks to focus on core competences, leaving the commercial sector to develop and optimize service experiences for customers. This public-private approach helps encourage competition, efficiency, and innovation in payments. The central banks of China[27] and Sweden[28] are experimenting with a two-tier structure, and the Bank for International Settlements[29] supports it.

> **"History indicates that the most effective and efficient payment system is a two-tier one."**
>
> Bank for International Settlements

Two-tier CBDC architecture



Account-based, token-based, and bearer instrument approaches

In account-based models, the CBDC system maintains records of user account balances. In a two-tier approach, users access their CBDC through PSPs that authenticate their identity and maintain account records.

Token-based models operate in a similar way but by recording ownership of each CBDC token. An important difference is that a CBDC transfer can involve multiple tokens. As a result, a token-based system may need more IT resources than an account-based one to complete a transaction. Although blockchain technologies are often associated with token-based systems, you can implement token-based systems without blockchain.[30] You can also use blockchain in account-based models.[31]

A bearer instrument model is a specific token-based approach that does not need to maintain ownership records for tokens, and token holders don't need to prove ownership to use them. Therefore, users can transact with CBDC anonymously, in a similar way to physical cash. If a central bank adopts a bearer instrument approach, they need to consider security-driven limitations around fully anonymous transactions. There are also concerns that users are at greater risk of losing CBDC if their digital wallet or account becomes unavailable.

Offline operation

For a CBDC to replicate the characteristics of physical cash, it needs to support offline transactions. That way, people can still use it if the connection to the core ledger or PSP is unavailable or if identities/fund availability can't be verified. While PSPs could programme devices like smartphones to support offline transactions, they would need to operate in a secure way, maintaining the integrity of CBDCs held in accounts or digital wallets.[32] They would probably also need to store offline transaction data, so they could share it with the CBDC system when back online.

The CBDC solution must also consider risks like token counterfeiting and account manipulation. So central banks will want to limit offline transaction values. This could require digital signatures from both parties to confirm an offline transaction history (as in the People's Bank of China "dual offline" wallet system[33]). It could also include limits on the number of offline transactions or limits on the time a device can be offline.

Clearing and settlement models

In a two-tier CBDC system which executes transactions online, there are three ways PSPs can communicate to clear and settle transactions.

Pre-clearing stage between PSPs before settlement

Here, PSPs manage CBDC account/token records and then communicate with each other to execute and clear transactions. One advantage of this approach is that it's not wholly dependent on the CBDC core ledger system. This is helpful if settlement processing takes longer than anticipated or the CBDC system is unavailable. Although the transfer recipient could not use the funds until after settlement, the transaction would be guaranteed as soon as clearing takes place.

Direct settlement

In this model, the CBDC system settles transactions directly without any prior communication taking place between PSPs.

An advantage of this model is that it could broaden the ecosystem of PSPs operating within the system. The key disadvantage is it lacks a pre-clearing stage. This means there could be more failed transactions due to payment detail errors.

No reference to any centralized CBDC for clearing or settlement

In this third approach, communication with the central bank is only to ensure complete transaction records for monitoring and economic analysis. The CBDC is token-based and operates as a bearer instrument, but PSPs can be involved in processing transactions online. The solution developed by eCurrency Mint Limited[34] uses this model.

Network architecture options

There are two main network architecture options for clearing. Each aligns to approaches currently used for real-time gross settlement (RTGS) and fast payment systems (where payment message transmission and final fund availability occur in real-time/near real-time on as close to a 24/7 basis as possible[35]).

Hub model

With this model, messages between PSPs to clear transactions pass through a central hub. Once clearing is complete, a message goes to the CBDC system so settlement can occur.

Settlement could take place offline, similar to the UK Bankers Automated Clearing Service (BACS) system for large inter-bank payments. More commonly, settlement will occur online at the same time as clearing, similar to the RTGS system in Singapore and the TARGET Instant Payment System (TIPS) across Europe.

Payment systems based on the direct settlement model also use the hub network architecture. There's no transaction pre-clearing between PSPs before settlement and no need for any network connection between PSPs. The SPEI RTGS system in Mexico[36] uses this approach.

Distributed model

Here, messages go directly between PSPs to clear the transaction. The network enables direct communication between PSPs and with a centralized settlement system. SWIFT operates a network like this, which the New Payments Platform in Australia uses for its RTGS system.[37]

A final consideration is whether messages can go through the Internet or need a private network connection. Generally, private network connections like AWS Direct Connect will be preferred because they offer greater performance consistency. However, in some situations, the Internet may be acceptable using a suitable secure protocol.

PSP roles and interoperability

Let's look at the roles and functions involved in operating payment transactions and related services. Taking existing commercial banking payment methods (like credit card payments or inter-bank transfers) as a starting point, we'll discuss how they could map to different PSP roles in a CBDC system. See infographic "CBDC PSP ecosystem" on page 14.

Account management

This role is responsible for maintaining CBDC ownership records (such as account balances and transactions) and providing various overlay services that benefit customers (such as access to information through mobile devices). Another important function is managing transactions—transferring money and accepting payments on a customer's behalf.

These functions can be replicated essentially unchanged in a CBDC solution, whether it's account-based or token-based. As with existing commercial bank account providers, there would need to be strict regulatory oversight, including the application of standards, controls, and regulatory accountability in identity verification, AML, and fraud detection.

However, there's a key difference in how existing commercial banks operate and how PSPs would operate in a CBDC model. In a CBDC model, PSPs don't record sums in accounts they manage on their balance sheet. The money in a CBDC account isn't a debt the PSP owes the account holder—it's the central bank's liability. This means an account management PSP does not need to hold reserve accounts with the central bank and is not subject to the same capital requirements as a commercial bank. As a result, a wide range of market participants could fulfill the account management PSP role.

Payment initiation services

In addition to account management, PSPs could provide services to capture a transaction (either online or at a merchant location) and initiate a transaction using CBDC. This role is similar to that of payment gateway service providers in existing card payments systems.

Identity verification

The account management PSP or account holder would appoint a PSP responsible for identity verification. This PSP would interact with the account management PSP through APIs defined and governed by the central bank. The PSP could use their own identity verification function based on standardized specifications or operate a centralized system for ID credentials.

Unlawful activity prevention

Separate PSPs could be responsible for AML and fraud detection.

Programmable money support

A CBDC solution can enable programmable money where a transaction is executed but payment isn't settled until certain conditions are met. A mutually trusted authority must determine the condition status before the transaction is executed. This could be a PSP operating as an oracle.[38] The transaction parties would agree on the oracle PSP appointment.

The oracle's role is to provide definitive information on the status of transaction conditions.

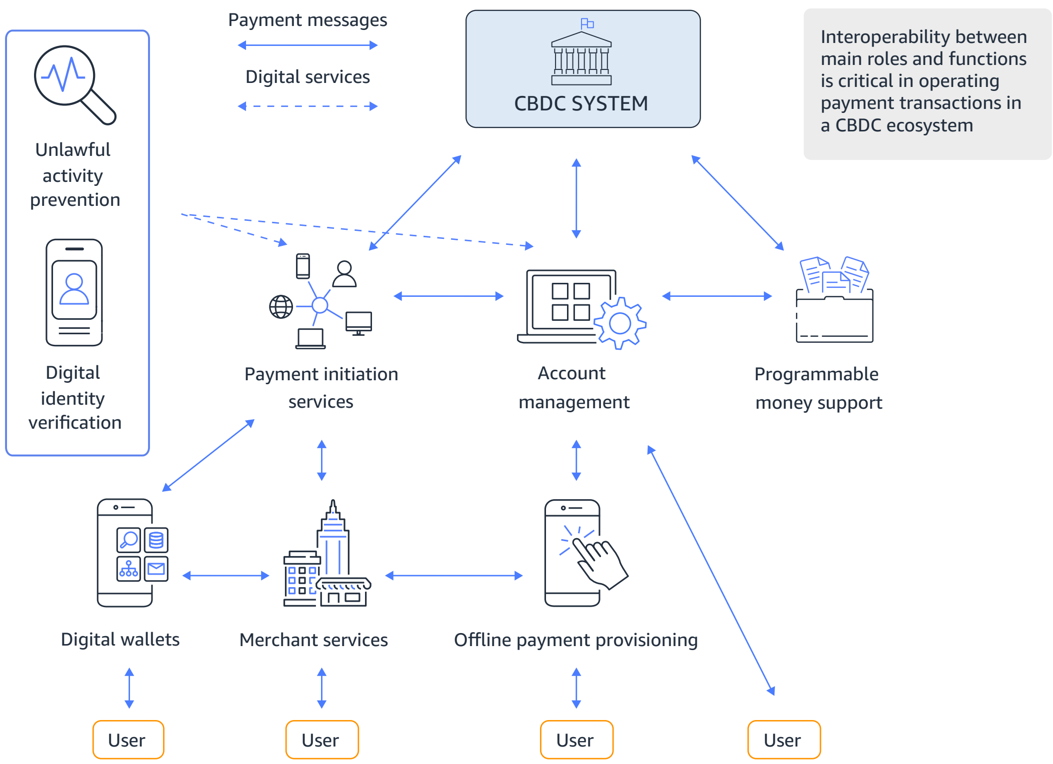
Offline payment provisioning

Both account-based and token-based CBDC models can support limited offline transactions. PSPs could provide this capability through dedicated devices or a smartphone application, which would have security features to prevent tampering.[39]

Offline transfers from the device/application would need to comply with defined central bank protocols, such as the use of QR codes or NFC communication. Transfers could also require additional security, like user pin codes.

The CBDC system would then inspect the offline transaction history when the device is back online, with the CBDC traced back to the PSP that originally moved it to the device for offline use. At this point, the PSP would be responsible for certifying there was no double spend.

CBDC PSP ecosystem



Conclusion

In this paper, we have looked at CBDC objectives and their implications for CBDC design and architectural principles.

To support the objective of improving payment system resilience and competition, we recommend a two-tier, general purpose CBDC where a PSP ecosystem provides services to individuals.

To prevent unlawful activity, a CBDC system based on online transactions (either token- or account-based) offers more benefits than a fully offline bearer instrument approach. However, to support the objective of financial inclusion, you need offline capabilities that replicate the benefits of physical cash. Both account-based and token-based models can support this through PSPs using secure devices and identity authentication methods.

PSPs can also provide services that enable smart contract and programmable money functionalities, accelerate innovation, and expand financial inclusion by delivering and innovating payment services, identity authentication methods, and unlawful activity detection efforts. The enablement of a PSP ecosystem is key to achieving central bank objectives.

Finally, we conclude that if improving cross-border payments is a priority, both wholesale and general purpose CBDCs offer potential solutions.

See "CBDC (part 2): Technology options and performance criteria" for a recommended reference architecture designed to meet key technical performance criteria for a fully-functional CBDC solution.

Read now

Looking to take the next step?

No matter where you are in your journey to the cloud, we are here to help. For more information, browse our technical resources to expand your knowledge of the AWS Cloud or contact us to connect with an AWS expert.

References

1 World Economic Forum, January 2020: Central bank digital currency policy-maker toolkit.
2 McKinsey & Company, September 2019: Global payments report 2019: amid sustained growth, accelerating challenges demand bold actions.
3 Sveriges Riksbank report, 2 October 2018: The Riksbank e-krona project report 2.
4 Bank for International Settlements report, November 2019: Shaping the future of payments.
5 Hyperledger.org case study, August 2020: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha.
6 AWS solutions paper, 2020: SGX uses Amazon managed blockchain to build innovative payment solution.
7 Financial Stability Board, 13 October 2020: Enhancing cross-border payments
8 AWS publication, 2020: TransferWise grows globally by migrating financial applications to AWS.
9 SWIFT publication, August 2018: SWIFT payment controls: protecting your payment operations against fraudulent attacks.
10 European central bank, December 2019: Exploring anonymity in central bank digital currencies.
11 Hyperledger.org case study, August 2020: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha.
12 Binance Research report, August 2019: First Look: China's central bank Digital Currency.
13 Sveriges Riksbank report, February 2020: The Riksbank's e-krona pilot.
14 Special chapter in Bank for International Settlements 2020 annual economic report, 24 June 2020: Central banks and payments in the digital era.
15 eCurrency Mint Limited publication, 2017: The case for digital legal tender: the macroeconomic policy implications of digital fiat currency.
16 Hyperledger.org case study, August 2020: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha.
17 Bank of Canada Staff Analytical Note, June 2020: Designing a CBDC for universal access.
18 News reports including 8BTC article, February 2020: Three schemes for dual offline payment of CBDC, says China's central bank.
19 eCurrency Mint Limited publication, 2017: The case for digital legal tender: the macroeconomic policy implications of digital fiat currency.
20 Bank for International Settlements report, March 2020: Fast retail payment systems.
21 Banco de Mexico publication, March 2016: Interbank Electronic Payment System (SPEI)
22 Reserve Bank of Australia Bullet, September 2018: The new payments platform and fast settlement service.
23 Various publications including: Medium, Blockchainhub and Chainlink.
24 SWIFT publication, August 2018: SWIFT payment controls: protecting your payment operations against fraudulent attacks.
25 European central bank, December 2019: Exploring anonymity in central bank digital currencies.
26 Hyperledger.org case study, August 2020: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha.
27 Binance Research report, August 2019: First Look: China's central bank digital currency.
28 Sveriges Riksbank report, February 2020: The Riksbank's e-krona pilot.
29 Special chapter in Bank for International Settlements 2020 annual economic report, 24 June 2020: Central banks and payments in the digital era.
30 eCurrency Mint Limited publication, 2017: The case for digital legal tender: the macroeconomic policy implications of digital fiat currency.
31 Hyperledger.org case study, August 2020: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha.
32 Bank of Canada Staff Analytical Note, June 2020: Designing a CBDC for universal access.
33 News reports including 8BTC article, February 2020: Three schemes for dual offline payment of cbdc, says China's central bank.

34 eCurrency Mint Limited publication, 2017: The case for digital legal tender: the macroeconomic policy implications of digital fiat currency.
35 Bank for International Settlements report, March 2020: Fast retail payment systems.
36 Banco de Mexico publication, March 2016: Interank Electronic Payment System (SPEI).
37 Reserve Bank of Australia Bullet, September 2018: The new payments platform and fast settlement service.
38 Various publications including: Medium, Blockchainhub and Chainlink.
39 Cornell University Publication, 14 December 2020: Towards a two-tier hierarchical infrastructure: an offline payment system for central bank digital currencies.