BIS Innovation Hub

Project Icebreaker

Breaking new paths in cross-border retail CBDC payments

March 2023

Bank of Israel

NORGES BANK

Sveriges Riksbank

Content

Foreword

Project Icebreaker explores the potential benefits and challenges of using retail CBDC in cross-border payments. It tested the technical feasibility of conducting cross-border/cross-currency transactions between different DLT-based CBDC proofs of concept. The aim was to gain a deeper understanding of the technologies used, and to identify the key technical and policy choices and trade-offs that central banks would need to consider in designing CBDC implementations that facilitate cross-border payments. The project was a collaboration between the Bank of Israel, Norges Bank, Sveriges Riksbank and the BIS Innovation Hub.

"*If Israel is to issue a digital shekel, it would be very important that we do it according to the evolving global standards, so that Israelis could use it for efficient and accessible cross border payments. While there is still much work ahead of us for the Icebreaker model to become a global standard, the learnings from this successful project have been very important for us and for the central banking community. I thank the BIS Innovation Hub, the colleagues from the Riksbank and Norges Bank, and our devoted professional staff here at the Bank of Israel for the effective collaboration and the professional work.***"**
Andrew Abir, Deputy Governor, Bank of Israel

"*We are delighted to have been part of one of the first experimental tests of cross-border retail CBDC payments, together with our partners the BIS Innovation Hub, Sveriges Riksbank and Bank of Israel. This project contributes to the important global effort to improve cross-border payments. In addition, it has added significant value to Norges Bank's experimental test of a domestic system for retail CBDC payments.*"
Torbjørn Hægeland, Executive director for Financial Stability, Norges Bank

"Although domestic payments have become less expensive, safer and more efficient, payments across currencies are still associated with high costs, slow speed and risk. When exploring CBDCs it is important to include cross-currency opportunities from the start. Project Icebreaker shows how different CBDC solutions in different countries could enable instant cross-currency transactions in a way that would greatly benefit the end users. The project has also been a great example of collaboration and sharing of knowledge between the participating central banks and BIS. Although there are a lot of questions that need to be investigated further, Project Icebreaker is a valuable initiative and contribution to the discussion on how we can improve cross-currency payments."
Aino Bunge, Deputy Governor, Sveriges Riksbank

"*Project Icebreaker is yet another example of the value of the practical and quick experimentation needed to advance the learnings and thinking required for implementations of retail CBDC systems so that key functionality, such as enabling cross-border and cross-currency payments, can be designed from the outset. The project demonstrated how such functionality could be achieved with minimal requirements on national CBDC systems as well as enabling easier integration and interoperability between them. The Icebreaker model also demonstrated other benefits for everyday users such as increased transparency, lower costs, increased competition*

and lower risks. More work is still required for retail CBDC but the learnings from this project are invaluable for central banks. The fast paced, focused and collaborative spirit across the Riksbank, Norges Bank, Bank of Israel and the BIS Innovation Hub is something the teams involved should be proud of."
Beju Shah, Head of the BIS Innovation Hub Nordic Centre.

1. Executive summary

While domestic payments have seen significant improvement in many jurisdictions in recent years, cross-border payments still face challenges such as high costs, low speed, limited access and insufficient transparency. The G20 has made it a priority to enhance cross-border payments and, in response to this call for action, the BIS Innovation Hub is coordinating experiments on how this might be done.[1, 2]

Many central banks are exploring retail central bank digital currencies (rCBDCs). Some of these projects are at the proof-of-concept (PoC) stage, while others are in pilot trials and a handful have reached more mature phases.[3] The requirements for interlinking these (domestic) rCBDC systems to support cross-border payments should be considered at the outset so that cross-border payments can be enabled when appropriate.

Project Icebreaker explores a specific way to interlink rCBDC systems (the hub-and-spoke solution) with several additional features that would allow the Icebreaker model to be readily scaled up. In addition, these features would promote simplicity and interoperability, reduce settlement risk, and foster competition and transparency for cross-border rCBDC payments.[4]

Settlement risk and speed. In the Icebreaker model, a cross-border transaction is broken up into two domestic payments, one in each domestic system. An rCBDC therefore never leaves its own domestic system. This is because FX providers buy one currency in one system and sell the other currency in the other system. An FX provider therefore holds rCBDC supporting wallets in two or more systems. Settlement is via an atomic payment-versus-payment (PvP) arrangement using Hash Time Locked Contracts (HTLC), which can be thought of as similar to a digital escrow. This eliminates the time gap between payment initiation and settlement, going a long way towards eliminating counterparty risk in the FX transaction.

Competition and transparency. In most existing cross-border payment systems, the end user is bound to its payment service provider (PSP) for FX service. In the Icebreaker model, the FX service and pricing are decoupled from

---

1 Cross-border payments have been on the agenda of international bodies and standard setters for several years. The G20 Roadmap lays out a comprehensive set of actions covering 19 building blocks. The Committee for Payments and Financial Infrastructure (CPMI) leads the implementations of building blocks 11–19, where building block 19 explores the use of CBDC for cross-border payments. For more information, see CPMI Cross-border payments programme (bis.org).

2 For the BIS Innovation Hub coordinating experiments, see BIS Innovation Hub (2022).

3 CBDC is central bank-issued digital money denominated in the national unit of account and constituting a liability of the central bank. A retail CBDC is available to the public for use in payments. See Kosse and Mattei (2022) for an overview of central bank activity in CBDC.).

4 Beside the features of the Icebreaker model, the use of risk-free money central bank money held directly by end users reduces credit risks and the need for some financial intermediaries therefore reducing counterparty risks. For more on interoperability between CBDC systems in a cross-border context, see CPMI et al (2022).

the provision of rCBDC payment services. FX providers submit FX rates to the Icebreaker hub, which selects the best rate to be presented to the payer for each payment request. This lets the payer access competitive FX rates independently of the PSP providing the end user with a digital rCBDC-supporting wallet. Additionally, the risk of insufficient liquidity in the desired bilateral currency pair is mitigated not only by the presence of multiple FX providers, but also by using bridge currencies. This could have potential in promoting competition between FX providers and making FX fees more transparent for end users.

Interoperability and scalability. The number of connections between rCBDC systems are kept to a minimum by the hub-and-spoke approach used for the Icebreaker model. The Icebreaker hub only routes payment messages and does not act upon them. The only information it acts upon is the data from FX providers, which are used when identifying and selecting the best FX rates for the payer.

The Icebreaker model makes a minimal set of technical requirements about the rCBDC systems that connect to it, namely that:

- Each must be a functioning payment system and operate in real time, or near real time, ideally 24/7/365.
- Each can implement and support the use of HTLC.
- There are participants in each rCBDC system that can act as FX providers.

The Icebreaker hub provides a standard set of application programming interfaces (API), enabling different domestic systems to communicate with it seamlessly. The technological requirement on domestic systems is deliberately kept to a minimum, thus promoting scalability, interoperability and simplicity.

The project focused on core features only, including the technical solution for the Icebreaker hub, the integration of the three PoC rCBDC systems of Israel (Ethereum Quorum), Norway (Hyperledger Besu), and Sweden (Corda), and the technical validation of a limited set of key use cases, together with related policy considerations.[5] Functional aspects such as AML/CFT, or longer-term considerations such as the business model or scheme rulebook were deemed out of scope but could be considered in future experimentation.

Project Icebreaker shows that central banks can have almost full autonomy when designing their domestic rCBDC system while still being able to participate in a formalised interlinking arrangement to enable cross-border payments.

The key recommendations for a central bank considering enabling cross-border payments in an implementation of a rCBDC system are to:

[5] See Appendix A for a high-level description of the three rCBDC PoCs. They were built for the purpose of conducting experimental tests and should not be taken as indicative of any future rCBDC design decisions on the part of the participating central banks.

- Consider ways to incorporate conditional settlement, eg HTLC.
- Consider ways to ensure system availability and short response times 24/7/365 to maximise speed and minimise failed payments.
- Consider adopting current messaging and addressing standards and ensure flexibility in adopting future standards.
- Consider ways to provide instant rCBDC liquidity for FX providers 24/7/365.
- Promote transparent and competitive incentives for FX providers.

Implementing the Icebreaker model in the real world would require a range of technology, policy and legal considerations to be addressed. Policy considerations could include the governance arrangement, the viability of the business model, liquidity provision, privacy, AML/CFT compliance and monitoring, and payment initiation-related standards. Legal considerations would include a sound legal basis for the Icebreaker hub type approach, as well as the potential for conflict of laws and regulations between connected rCBDC systems, and conflict resolution. Technical considerations could include resilience requirements for the Icebreaker hub and participants in the rCBDC systems. Central banks should factor in such cross-border aspects into the design of their rCBDC systems to avoid creating unintended barriers for cross-border functionality. The Icebreaker model could serve as a platform for introducing payments innovations (such as delivery versus payment and programmable money use cases) that countries could consider in the context of developing the cross-border capabilities of their CBDC systems.

2. Definitions, acronyms, and abbreviations

2.1 Definitions

Bridge currency: A currency that is used as an intermediate step in an exchange between two currencies for which there is no direct FX rate, or the FX rate is unfavourable.

Foreign exchange (FX) provider: Entities that provide the service of exchanging rCBDC in one currency into rCBDC in another currency. They buy one currency using their rCBDC wallet in one rCBDC system and sell the other currency using the wallet in the other rCBDC system.

Hash function: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. The values returned by a hash function are called hash values, hash codes, digests or simply hashes.

HTLC: A hash time-locked contract (HTLC) is a type of smart contract used in DLT applications to reduce counterparty risk by creating a time-based escrow that requires a cryptographic passphrase to unlock it.

Interoperability: The technical, semantic and business compatibility that enables a system or mechanism to be used in conjunction with other systems. Interoperability allows participants in different systems to conduct, clear and settle payments or financial transactions across systems without participating in multiple systems.

Payment-versus-payment (PvP): A settlement mechanism that ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place. If more than two currencies are involved in a PvP chain, it is called **PvPvP** in the context of this study.

Retail central bank digital currency (rCBDC): A digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank and available to the public.

rCBDC system: An rCBDC ecosystem would comprise multiple elements and functions. A core ledger with supporting infrastructure and rules would underpin a broader ecosystem of processing infrastructure, wallet providers and user services with business and technical rules.

SHA-256: SHA stands for Secure Hash Algorithm and 256 is the number of bits in the output of the cryptographic process. SHA-256 is a member of the SHA-2 family consisting of six hash functions created by the US National Security Agency.

Wallet: Electronic wallets are payment arrangements that enable end users to securely access, manage and use a variety of payment instruments issued by one or more payment service providers via an application or a website. The electronic wallet may reside on a device owned by the holder, eg a smartphone or a personal

computer, or may be remotely hosted on a server but still under the control of the holder.

Wallet provider: An entity that provides electronic wallets to the general public and typically has a licence to provide payment services and can include both banks and non-banks such as fintech companies.

2.2 Other acronyms and abbreviations

AML	anti-money laundering
API	application programming interface
BIS	Bank for International Settlements
CFT	combating the financing of terrorism
CPMI	Committee on Payments and Market Infrastructures
DID	decentralised identifiers
DLT	distributed ledger technology
FX	foreign exchange
KYC	know your customer
PFMI	Principles for financial market infrastructures
PSP	payment service provider
PoC	proof of concept
RTGS	real-time gross settlement

3. Introduction

Project Icebreaker makes a practical contribution to the debate on the use of rCBDCs in cross-border payments (which, for the purposes of this project, also include cross-currency payments). This experiment helps to identify the key technical and policy choices that central banks may need to consider in their rCBDC exploration.

To date, the BIS Innovation Hub cross-border CBDC projects have explored a variety of approaches to improving cross-border payments. Project Jura, Dunbar, and mBridge explored multilateral platforms on which several wholesale CBDCs are issued.[6] Project Icebreaker explores an alternative approach using a hub-and-spoke solution to interlink different rCBDC DLT-based systems. While Project Icebreaker has some similarities with Project Nexus, which interlinks domestic instant payment systems, it is distinct in its settlement method, the choice of FX provider, the use of bridge currencies and the technologies used in each domestic system.[7]

This report describes the model used in this project, the payment process (Section 4), the Icebreaker hub's solution design, technical architecture and the experiments conducted, as well as the key findings and lessons learned (Section 5). Policy considerations are presented in Section 6 and Section 7 concludes.

4. Overview of the model used for Project Icebreaker

This section provides an overview of the model used in Project Icebreaker, which consists of the domestic rCBDC systems, the FX providers, the Icebreaker hub and the payment process, (see Graph 1). Technical considerations, design choices and policy considerations are detailed in later sections.

4.1 Domestic rCBDC systems

rCBDC systems, at their simplest, consist of different layers and participant types. As such, they are evolving ecosystems. An rCBDC system is consequently a broader concept than the technical core infrastructure provided by a central bank.[8]

At the system's centre would be the central bank providing the core technical infrastructure for, at a minimum, issuing and redeeming rCBDC. The core infrastructure would typically be complemented by a scheme and a rulebook that specifies rights and responsibilities as well as the relevant technical, security and

6 See BIS Innovation Hub (2022) and CPMI et al (2023).

7 See BIS Innovation Hub (2021) for Project Nexus.

8 For a more detailed discussion of the design of CBDC systems, see eg BIS et al (2021a).

data messaging standards and other operational and legal requirements for system participants (out of scope for this project).

In the next layer are the wallet providers. As banks or non-banks such as fintech companies licensed to provide payment services, they provide end users with wallets supporting rCBDC. They serve as a distribution layer between the central bank and the end users through which the end users can receive, hold, and transact using their rCBDCs.

In the outer layer are the end users, which can be individuals or private or public sector entities. They participate as payers and payees using rCBDC services.

4.2 FX providers

The Icebreaker model facilitates cross-border payments by interconnecting rCBDC systems. FX providers, who are members of multiple rCBDC systems, would exchange rCBDC in one currency for rCBDC in another currency. In essence, they would buy one currency in one rCBDC system paying with the other currency in the second system. If Alice in Sweden wanted to pay Bob in Israel, the FX provider would buy Swedish krona and sell Israeli shekel. An FX provider could be any entity, eg a financial institution holding wallets in two or more rCBDC systems, that is willing to take on FX risk to facilitate payments.[9] The cost of holding and managing liquidity would, together with the FX risk, be reflected in the spread between the buy and sell rates offered for each specific currency.[10]

4.3 The Icebreaker hub

The Icebreaker hub performs two main functions:

- Routing cross-border payment messages between domestic systems.
- Providing a "marketplace" matching payers with FX quotes from FX providers.

To fulfil its role, the Icebreaker hub makes a minimum set of requirements for each domestic system:

- that it must be a functioning payment system and operate in real time, or near real time, ideally 24/7/365,
- that it can implement HTLC (see Section 5.3.1), and

[9] An entity that acts as wallet provider could also act as FX provider. However, this is not necessarily the case, and for the remainder of the report, FX and wallet providers are referred to as separate functions.

[10] One simplifying assumption in Project Icebreaker is that the FX provider has adequate liquidity at the given rate.

- that it has participants who are serving as FX providers.

4.3.1 A hub-and-spoke solution

There are several ways of interlinking disparate systems. Single access, bilateral linking and "hub-and-spoke" solutions are all alternatives to single common platform models.[11] Project Icebreaker explored a hub-and-spoke solution interlinking domestic systems through a technical platform that facilitates communication between rCBDC systems. Each rCBDC system needs only to integrate with one external system (the Icebreaker hub), rather than integrating with every other individual rCBDC system. The advantage of this model is that it can scale up to support many participating systems without increasing the complexity of the design, given the total number of connections between rCBDC systems that would need to be configured once the network starts growing.[12]

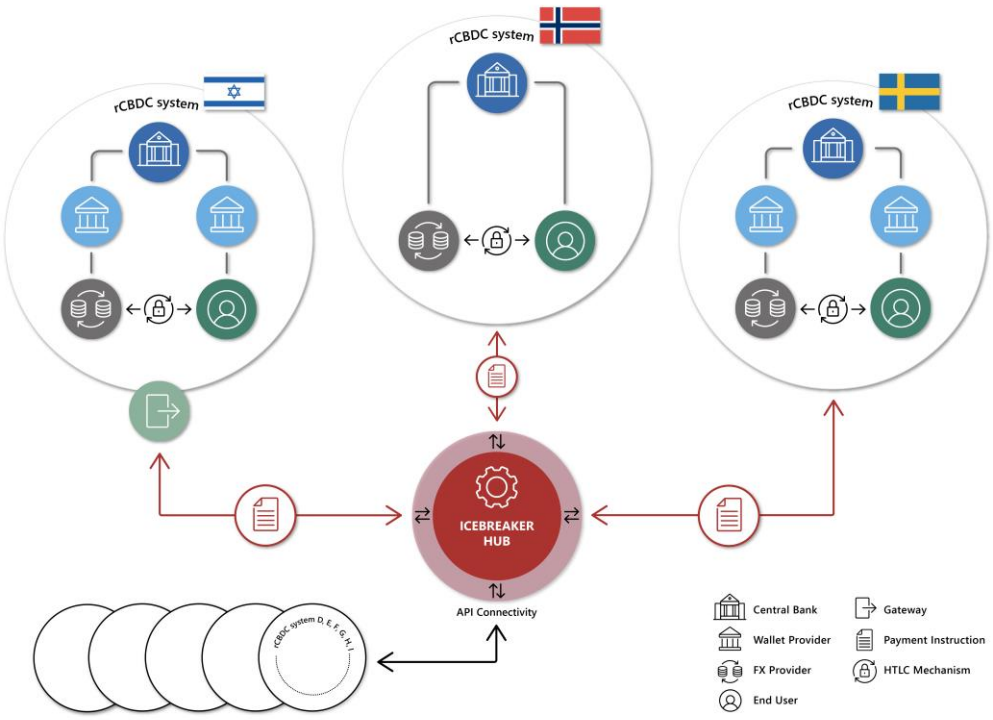
Each domestic rCBDC system can connect to the hub in two ways, each having different effects, some of which are out of the project's scope. The first is to let the system participants, such as wallet and FX providers, communicate with the hub directly. The second is that the domestic rCBDC system provides a gateway to serve as a single communication channel between the domestic rCBDC system and the hub.

---

11 See CPMI et al (2022).

12 With *n* rCBDC systems, *n* connections are sufficient in the hub-and-spoke model, while solutions without a central hub require at least *n(n-1)/2* such connections. For 15 countries, 105 connections are needed without a hub-and-spoke solution (making the network topology very complex and error-prone, as well as increasing cyber security risks) but this comes down to 15 with the hub-and-spoke model.

Graph 1. A high-level view of the Icebreaker model.



Note: The domestic rCBDC systems in the graph have different distribution models to illustrate that design and technology choices can differ between rCBDC systems in the Icebreaker model. The illustration is inspired by the three PoCs in the experiment. Moreover, the FX provider is here assumed to use a wallet provider for its FX wallet. This may not always be the case, and an FX provider may be its own wallet provider.

4.3.2 FX marketplace

As described earlier, FX providers would hold and manage rCBDC liquidity in their operating currencies. Each FX provider would submit buy and sell rates for those currencies to the Icebreaker hub. The Icebreaker hub therefore maintains a live database of the submitted FX rates and returns the best available rate along with the identity of the FX provider to the payer upon request. This function of the Icebreaker hub is similar but not identical to the model in Project Nexus and could be described as a FX "marketplace" (see Section 5.1 for more details).

4.4 The payment process

A cross-border payment is divided into two domestic payments. The payer pays the FX provider in the payer currency (the currency in the payer's rCBDC system), while the FX provider pays the payee in the payee's currency (the currency in the payee rCBDC system). No rCBDC leaves its own jurisdiction. The cross-border payment is executed in such a way that the payee will only receive its money if it gives the FX provider the information necessary to claim its money from the payer. Therefore, the

payer will only pay the FX provider if the FX provider has paid the payee. In this report, this is referred to as "coordinated settlement in PvP style" (see Section 5.1).

The communication via the Icebreaker hub is enabled by APIs, which let it interoperate in a standardised way with each PoC rCBDC system. Below, transactions are described in terms of the payer's or payee's wallet performing certain tasks. This is a simplification. Depending on the individual domestic rCBDC technology solution, the task is performed either by the wallet or by the wallet provider on behalf of the wallet's owner.

The four stages of the payment process are:

Stage 1 (Get quote): The payer opens the wallet and inputs the payee country and the amount to be paid. This amount can be determined in either the payer or payee currency.

- The payer wallet sends a request for a quote to the Icebreaker hub (step 1 in Graph 2).
- The Icebreaker Hub retrieves the best available quote from the hub's database (step 2).
- The Icebreaker hub responds with the best quote and reports the identity of the FX provider back to the payer wallet (step 3).

Stage 2 (Payment discovery): If the payer accepts the quote (step 4), it proceeds by entering the payee's "payment address/alias". This requires the payer to have the relevant address information, which could be known by the payer in advance or may have been included in an invoice, an email, a scanned QR-code or other such medium.

- The payment request goes from the payer wallet via the Icebreaker hub to the payee wallet (step 5).
- The payee wallet validates its wallet address and generates a secret, eg a number or a phrase (step 6). A specific feature in the Icebreaker model is the use of locked (conditional) payments enabled by HTLC. The secret generated in this step will later be used to unlock the locked payments. The payee wallet generates an encryption (hash value) of the secret, and this hash value will be used to lock the payments in the next stage. This is explained below in Section 5.3.1.
- The payee wallet sends the address verification result and, if successful, the hash value through the Icebreaker hub to the payer wallet (step 7).

Stage 3 (Payment setup): The payer now initiates the payment.

- The payer wallet creates a locked (domestic) payment from the payer wallet to the FX provider's payer currency wallet (step 8).[13]

- The FX provider's payer currency wallet sends the payment information and the hash value to the FX provider's payee currency wallet via the Icebreaker hub (step 9).

- The FX provider's payee currency wallet creates a (domestic) locked payment in the payee currency to the payee wallet (step 10).

Note that both payments are locked by the same hash value that was provided by the payee's wallet (step 7).

Stage 4 (Payment completion): The cross-border payment is completed by the unlocking of the locked payments.

- The payee wallet recognises that there is a locked incoming payment waiting to be unlocked. It checks the payment information and presents the secret generated in step 6 to the HTLC mechanism that has locked the payee currency payment (step 11).

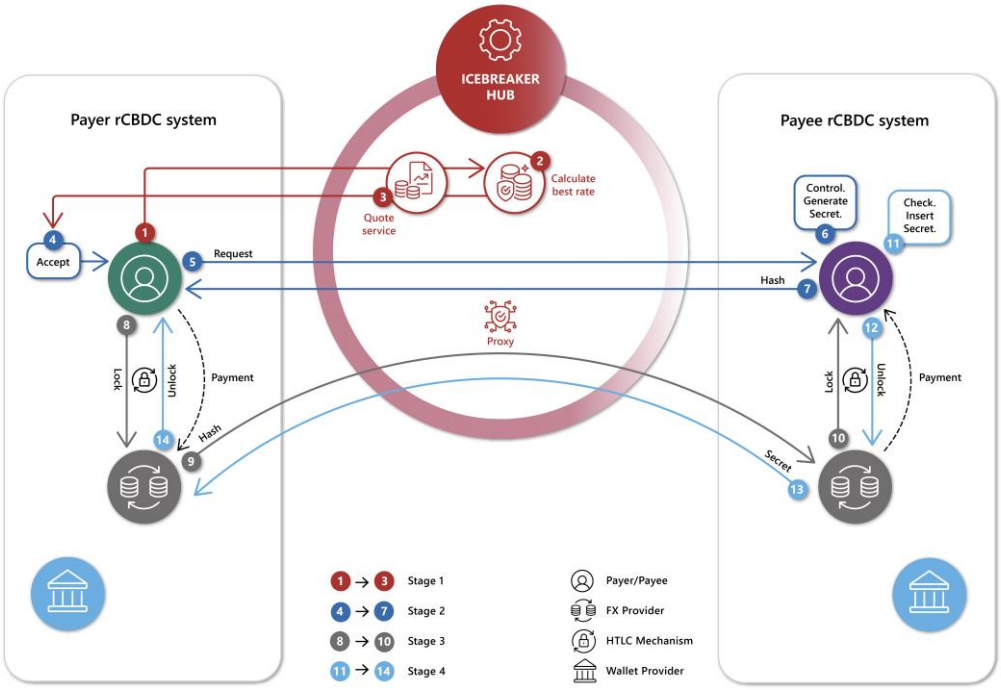
- The calculated hash value of the presented secret matches the hash value used to lock the payment. The funds are now released to the payee wallet (step 12).

- Because the payee currency payment has been unlocked, the secret is revealed to the FX provider's payee currency wallet (where the locked payment was located). The FX provider's payee currency wallet sends the secret, via the Icebreaker hub, to the FX provider's payer currency wallet (step 13).

- The FX provider's payer currency wallet uses it to unlock the incoming payer currency payment (step 14).

[13] Note that the payment from the payer to the FX provider is a domestic payment and that the FX provider is informed about it through the domestic CBDC system. The hub is used only to route messages across borders.

Graph 2. An overview of the payment process.



Note In the graph, the payment process is described as if it is the payer's or payee's wallet performing certain tasks. This is a simplification. Depending on the individual domestic rCBDC technology solution, a task is performed either by the wallet or by the wallet provider on behalf of the wallet's owner. The wallet provider symbol represents this possibility.

Although there are several steps and messages are sent back and forth in each stage, the entire process was completed within a few seconds during the project's system testing.

5. The experiment and solution design

The payment process described in the previous section highlights three key components of the model used in Project Icebreaker:

- How the payer receives the best FX quote.
- How communication between the different rCBDC systems is facilitated.
- How coordinated settlement in PvP style works.

These are described in more detail below, with an assessment of the advantages and disadvantages and possible alternatives. Following the test scenarios, the experiment's outcomes are set out.

5.1 The FX conversion mechanism

The Icebreaker hub maintains a database with FX rates uploaded by the FX providers. This design choice is intended to guarantee FX provision for end users, and to improve transparency and competition in FX provision by decoupling the FX services from the services provided by the wallet provider. An end user is not bound to a preferred FX provider that is selected by its wallet provider, unlike the situation in existing cross-border payments. The Icebreaker hub acts as an impartial broker. This design choice could also increase transparency for end users, who will know what the cost of the transaction will be, and who the FX provider is, before approving it.

The simulated payments in the experiment involved three currencies: the Israeli shekel (ILS), the Norwegian krone (NOK) and the Swedish krona (SEK). An FX provider could provide rates for any of the currency pairs, ie NOK/SEK, SEK/ILS and NOK/ILS. For each currency pair it is willing to trade, it can provide sell and buy rates (see Table 1 in Box A for an example). With three currencies in use, each FX provider can submit quotes for up to six rates.

Direct quotes for some currency pairs may be either unavailable or uncompetitive. Between small currencies, or country pairs with little or no trading, there may be no FX provider active in both currencies, or a sole FX provider may try to extract monopoly rents. In either situation, the Icebreaker hub will use a bridge currency to fulfil the FX need. For example, if no FX provider offers any service for the currency pair SEK/ILS, or if the FX rate is unfavourable, the Icebreaker hub would bridge this gap by determining an alternative payment route using NOK as an intermediary (bridge) currency. Only currencies participating in the Icebreaker arrangement can be used as bridge currencies.

The Icebreaker hub calculates the best effective rate, and the FX-rate quoted to the payer is always the rate of the cheapest payment route between the payer- and payee countries.[14]

[14] By the effective FX rate, we refer to the FX rate calculated on the final amounts in the payer's and payee's currencies.

Box A

A three-currency example

In Table 1, the Icebreaker hub would present the exchange rate of 1.10 from FX provider FXP2 to a payer who wants to make a payment from Sweden to Norway (and an exchange rate of 1.05 from FXP1 if the payer wants to make a payment from Norway to Sweden.

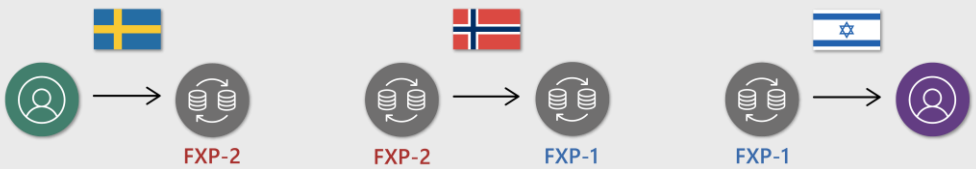
Table 1. Example of exchange rates in the Icebreaker experiment when two FX providers have wallets in all three rCBDC systems.

FX provider	Currency	FXP sell (Ask)	FXP buy (Bid)
FXP1	NOK/SEK	1.20	1.05
FXP2	NOK/SEK	1.10	1.00
FXP1	SEK/ILS	0.70	-
FXP2	SEK/ILS	0.50	-
FXP1	NOK/ILS	0.65	0.44
FXP2	NOK/ILS	0.54	0.40

Note: Red font indicates the best exchange rates. The first currency in a currency pair is the major currency and Ask and Bid rates are the rates at which the FX provider is selling or buying the major currency. For example, the NOK/SEK ask rate from FXP2 of 1.10 says that FXP2 sells 1 NOK for 1.10 SEK. The exchange rates are purely illustrative.

To illustrate how the Icebreaker hub can bridge gaps in the exchange rate table by using intermediate (bridge) currencies, assume that a Swedish payer wants to send money to an Israeli payee and that no FX provider can offer a Bid rate for the SEK/ILS currency pair, as in Table 1. The Icebreaker hub bridges the SEK/ILS gap by proposing NOK as the bridge currency. It identifies the rate from FXP2 (who demands 1.10 SEK for 1 NOK) as the best rate for exchanging SEK for NOK and the rate from FXP1 (who sells 0.44 ILS for 1 NOK) as the best rate for exchanging NOK to ILS. The bridge rate for SEK/ILS would then be 0.40=0.44/1.10.

Graph 3. Illustration of the use of NOK as bridge currency.



5.2 Communication and connectivity

The Icebreaker hub connects each linked rCBDC system through a standard interface via APIs. It does not act on the message content in any other way. Each message can be routed individually without requiring any knowledge of transaction history or data. This keeps the hub's technological requirements for domestic systems a minimum.

Without a hub-and-spoke approach, each rCBDC system would need to make individual specific network and infrastructure configurations to communicate with other rCBDC systems, eg by using IP address whitelisting or firewall configurations. Communication between these rCBDC systems may not be standardised via a common interface and would instead be a bespoke integration between each pair of rCBDC systems. This would be not only complex to support and maintain but could also introduce cyber security risks. The Icebreaker hub keeps the level of network and infrastructure configuration required to a minimum, thus simplifying and standardising the integration process for rCBDC systems.

Near real-time payments and a low rate of failed payments require payment messages between the Icebreaker hub and rCBDC systems to be synchronous, in the form of API calls. In practice, this requires the payer's and payee's wallets to reply and perform steps in the payment process (hosted wallets) on behalf of end users. An rCBDC system could, however, use, or allow for, unhosted (self-custody) wallets, where the wallet or the payee itself needs to take an action to accept a payment, with the risk of a failed payment if the required response time is not met. This problem could be mitigated by adjusting the timeout values for the API calls, but at the cost of reduced speed. Asynchronous messaging would be a better fit for cases where responses from a rCBDC system are not immediate and warrant further experimentation.

In the Icebreaker model, all cross-border communication is routed through the Icebreaker hub including messages between FX provider wallets. In practice, an FX provider is likely to have direct communication between its entities in different domestic systems. The authentication could be simpler and potentially more secure with direct communications within the FX provider's network than it would be via a proxied connection to the Icebreaker hub. On the other hand, direct communication between the FX wallets could constitute a risk for the overall cross-border arrangement as it would create operational dependency. Assuring a certain level of standards and governance for such communications would be harder than if communication between FX provider wallets were routed via the Icebreaker hub.

In practice, the ISO20022 standard would be used for the messages routed by the Icebreaker hub. In this experiment the ISO20022 standard was not used, but several of the data items align with business elements in the ISO20022 data dictionary whilst others may need to be introduced.

5.3 Coordinated settlement in PvP and PvPvP style

Many of the existing systems for cross-border payments are based on correspondent banking. A transaction via such arrangements can sometimes take several days, exposing the payer and the payee financial institutions to various counterparty risks. The best way to manage these risks is typically via PvP. In traditional PvP arrangements, both currencies are held on the same technical platform, and it is therefore possible to exchange both currencies simultaneously.[15]

Project Icebreaker investigates cross-border payments between rCBDC systems that are implemented on different solutions and achieve PvP or PvPvP without requiring a common technology or platform. This coordinated settlement in PvP style uses the FX provider as intermediary exchanging the two payments almost simultaneously.

Graph 4. Illustration of traditional PvP and coordinated PvP and PvPvP.

There are two approaches to providing such PvP across two different DLT-based ecosystems: HTLC and oracle-based. Oracle-based PvP relies on a trusted third party (ie the oracle) to coordinate the settlement, whereas with HTLC coordination is achieved by the technology solution.[16] This project opted for HTLC since it is aligned

[15] For more on the use of shared platforms in cross-border payments, see CPMI et al (2023).

[16] In an oracle-based design, the payer makes a conditional payment to the FX provider wallet in the payer rCBDC system. The condition here is that the oracle countersigns the transaction, and the oracle is trusted to do so if and only if the FX provider pays the payee. The oracle must be trusted by payer and FX provider, and it must also have presence in both rCBDC systems:

with the design choice for the Icebreaker hub to only route messages and not to play a more sophisticated role in the payment process.

5.3.1 The HTLC mechanism

Coordinated settlement is achieved using a HTLC pair, where one side locks the payment from the payer to the FX provider wallet in the payer currency, and the other locks the payment from the FX provider's wallet in the payee currency to the payee. Once established, the second stage is the unlocking of that conditional lock, so that the payment is released to the payee or back to the payer. The unlocking can happen in two ways: either the payee unlocks it to accept the payment by providing a secret before a fixed timeout (payment conditions are met), or the payer unlocks it after the timeout to claim the money back (payment conditions not met). In the first case, the conditional payment effectively succeeded and in the second it was effectively cancelled. In this experiment the timeout was set to one minute for each side.

The HTLC mechanism aims to establish the trust needed in the model used in this project and has the following benefits:

- The payer can be sure that its payment to the FX provider will go through if and only if the payee has received the correct amount.
- The FX provider can be sure that if the payment to the payee has been accepted, the payment from the payer will come through without fail.
- The payee can be sure that the payment received will match the payment information received during the payment discovery stage (see Section 4.4).

The secret can be any set of information, eg a number or a phrase. The hash value of a secret is an encryption of the secret that is easy to compute, although it remains impossible to compute the secret from the hash. By using the hashed secret in the conditional payment for locking, the secret remains safe but it is easy to verify whether a given secret is correct for unlocking because its hash value will be the same as the hash value in the conditional payment. During the experiment, SHA-256 was used as the hash-generating function.

Both payments are locked using the same hash value. This ensures that either both payments succeed (both can be unlocked by the same secret before they time out) or both fail (both time out).

In a real setting, the locking times need to be long enough to allow for a complete unlock. The risk of the FX provider not being paid is managed by allowing a locking time on the conditional payment from the payer to the FX provider's payer currency wallet that is sufficiently longer than the one on the FX provider's payee currency wallet to the payee. In general, short locking times pose the risk that cross-border payments will fail, and long locking times pose the risk that liquidity for the payer and the FX provider will be locked up for longer, imposing additional costs and restrictions on them.

For the payee, the sole risk is the acceptance and unlocking of an incorrect payment, which could happen only if there are issues with payee wallet, but this cannot arise from the use of HTLC. The risk could be mitigated by rules in a scheme rulebook where the payee accepts fulfilment of the payment instruction by unlocking the payment from the FX provider.

While the use of HTLC enables technology-based trust and safety, some parties still need to trust that other parties will behave honestly, eg between the end user and any wallet provider who could act on the end user's behalf (hosted wallets). A dispute resolution process would also be required for any erroneous cases that may occur.

5.3.2 Interactivity

The use of HTLC assumes that all involved wallets participate actively. This is unlikely to be a practical constraint for the payer or the FX provider wallets, but could be an issue for the payee. For example, the payee's wallet could be unavailable, or if a payment needs to be accepted manually, the payee might be unaware and fail to accept it. A less stringent requirement for payment message response time and a longer HTLC timeout could mitigate some of these risks but at the cost of a potentially longer payment process. The payer would also have to wait longer to initiate the payment if they do not know whether they can expect an immediate response from the payee wallet in the payment discovery stage.

Automated responses avoiding manual actions in the payment process is needed to ensure a low rate of failed payments and speed.

5.3.3 Bridge currency extension

The coordinated settlement process described above builds on the use of a direct payment route where the FX provider is active in both the payer and payee currencies. When a bridge currency is used, the coordinated settlement becomes slightly more complicated, even though the same underlying logic holds. In the example in Box 1 in Section 5.1, where the payment from Sweden to Israel uses NOK as a bridge between SEK and ILS, three conditional payments are needed instead of two:

- a conditional payment from the payer to FXP2 in SEK;
- a conditional payment in NOK from FXP2 to FXP1; and
- a conditional payment from FXP1 to the payee in ILS.

The "Get quote" and "Payment discovery" stages are the same, although the message load is now larger due to the additional information needed (eg the wallet addresses for the second FX provider). The "Payment setup" and "Payment completion" stages follow the same structure as before but have an intermediate step in the bridge rCBDC system, where an additional payment is made. The payment is completed when the payee first claims the ILS payment by revealing the

secret. This enables FXP1 to claim its payment in NOK, which, in turn, enables FXP2 to claim its payment in SEK.

In this example, to ensure that both participants bear the same level of risk, the timeout duration needs to be gradually longer closer to the end of the unlocking chain and relative to the number of currencies that are used in the transaction.

5.4 Test scenarios

The project tested three payment scenarios and cases.

Table 2. Overview of tested scenarios, cases, and validated items.

Payment scenarios tested	1. Payment between all combinations of countries when a direct path is available and most favourable. 2. Payment between Sweden and Israel using NOK as the bridge currency when no direct paths for (SEK/ILS) were available. 3. Payment between Sweden and Israel using NOK as the bridge currency when direct paths for (SEK/ILS) were available but were less favourable than the bridged path.
In all scenarios the project tested	1. Payment initiation can be denominated in either the payer currency or in the payee currency. 2. The function of the HTLC mechanism in the following situations: a. Payment was successful end to end. b. Payment was unsuccessful due to (a) payee did not unlock the payment before timeout was reached, or (b) FX provider lacked liquidity, causing one of the HTLC lock creations to fail.
For each test case, the project validated that:	1. The Icebreaker hub picked the best exchange rate(s), calculated the correct payment amount(s), and that the rCBDC systems generated the appropriate payment instruction to be executed. 2. The correct amount was locked in the payer's wallet when the HTLC lock was created on the payer's CBDC system. 3. For PvP, the correct amount was debited from the FX provider's wallet in the receiving CBDC system when the second HTLC lock was created. 4. For PvPvP, the correct amounts were debited from the two FX providers' wallets when the second and third HTLC locks were created. 5. In the case of a successful payment, the correct amounts were credited to the FX provider(s) and the payee's wallets. 6. In the case of an unsuccessful payment, the payer and the FX provider(s) had their wallet balances unchanged or restored to the value(s) before the payment was initiated.

In addition, the time duration for a payment to be completed was also measured, noting this is dependent on the domestic systems and the environment hosting the Icebreaker hub. In this experiment, payments, both PvP and PvPvP, were executed within a few seconds. These time durations could be shortened if performance optimisation was done for the domestic rCBDC systems and/or the Icebreaker hub. However, such time durations could also be prolonged where a participating rCBDC system takes longer to complete a transaction or the network connectivity was slower for one of the domestic rCBDC systems.

6. Policy considerations

This section sets out policy considerations that the central bank community may need to take into account when studying, investigating or engaging in an Icebreaker-type arrangement such as the one explored here. The considerations set out below should not be seen as exhaustive and may evolve if further work is undertaken.

6.1 Governance

The ownership and governance model, as well as the related trade-offs, for such an arrangement would need to be considered and set up in an optimal way. The arrangement could play a central role in cross-border rCBDC payments and would be expected to comply with the relevant provisions in the CPMI-IOSCO *Principles for financial market infrastructures* (PFMI).[17] This implies a transparent and effective governance structure and framework, including system rules, clear goals, effective decision-making processes, risk management policies and procedures, and clear rights and obligations. There should be a clear and sound legal basis for an entity operating such a hub. The governance structure should accommodate stakeholder involvement from multiple central banks, commercial participants, and several other types of actors.

The complexity of the governance structure is likely to increase with the number of stakeholders involved. On the other hand, involving stakeholders, such as central banks, has benefits such as legitimacy, balance of power, network effects, and alignment of incentives with social welfare, among others. For example, a lack of influence may deter central banks, wallet and FX providers from participating in such an arrangement. The network connected to a hub may be smaller than what would be considered as socially optimal, preventing the hub from generating the intended welfare improvement. A sufficient level of autonomy and control must be balanced with universality and standardisation.

6.2 Resilience

The hub-and-spoke solution implies that a hub could become a single point of failure. Operational disturbances could interrupt cross-border payment traffic routed via the hub. As a basis for the management of operational risks, relevant parts of the PFMI, including updates, as well as other industry standards for cyber security and

[17] The *Principles for financial market infrastructures* (PFMI), including amendments and additions, apply to all systemically important payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories. They set out requirements on legal basis, governance and risk management including financial and operational risks. The PFMI is the backbone of central bank oversight of FMIs and is also used by supervisors and international organisations such as the International Monetary Fund. For more information on the PFMI, see Principles for Financial Market Infrastructures (PFMI) (bis.org).

cyber resilience should be applied to a hub so that its operational resilience is robust. This may include specific requirements for disaster recovery and business continuity such as a second site, redundancy in power and communication, incident management plans and reserve routines.[18]

For transparency, institutions participating in a hub arrangement should be subject to publicly disclosed participation requirements. These should ensure that participants will be able to process payments under a specified range of conditions, in accordance with a hub's rulebook. The requirements could differ depending on the role of the institution within a hub arrangement.

6.3 The FX mechanism

The design of the FX mechanism could affect competition in the market for FX services and the complexity of the design of the hub. The model explored in this experiment is one option and other designs may be feasible and could be considered.

The proposed FX model, where payers are matched with FX providers offering the best quote, decouples wallet provision from the FX conversion service. A wallet provider with a large user base would not automatically receive the FX business of its user base, and FX providers would no longer be dependent on having a large user base to capture a large share of the market. While this model should increase competition in FX provision, potentially resulting in lower costs for end users, it may also reduce PSPs' incentives to be wallet providers as they would not automatically receive the FX business. On the other hand, the model explored in this project could lower the barriers for some PSPs to become wallet providers as they could provide this service without the costs associated with the provision of FX services.

In particular, the automated use of bridge currencies is an important feature.

- First, it could enlarge the network of connected rCBDC systems by enabling payments between countries where no direct FX services exist.

- Second, it could improve competition as direct FX services will compete not only with other providers but also with bridged FX services.

- Third, it could reduce liquidity costs for FX providers in that an FX provider would be able to reduce the number of currencies in which it is active. This could, over time, lead to efficiency gains such that most payments will use just a few common bridge currencies in liquid financial markets. As the

[18] For a stateless hub such as the Icebreaker hub, an industry-standard high-availability and geographically distributed deployment could be used to address operational resilience concerns, eg multiple hub servers in multiple data centres in different locations that dynamically (and transparently) routes traffic to an available server.

number of connected countries in the network grows, the potential use of a bridge currency, or multiple bridge currencies, increases.

Other extensions of the model used in this project are also possible. For example, the payer may receive several good rates and makes the choice itself. Alternatively, FX providers could have the option of posting different rates depending on the amount in question, eg to offer a volume discount. The benefits of such extensions should be weighed against the increased complexity of the hub's design.

If an error occurs in the selection of the FX rate, so that an economic loss or gain results for the payer, payee or FX provider, the hub's rulebook would need to define the allocation of risk among the involved parties clearly and transparently. The FX provider may, as an example, have an obligation to check that the stipulated exchange rate corresponds to the one posted and be liable for any losses that could arise from an undetected error.

6.4 Liquidity provision for FX providers

FX service providers are private profit-maximising entities holding liquidity in the respective currencies they deal in. If there is too little liquidity in one or more currencies, some payments may be delayed or not executed at all.

Central banks, because of their monetary policy and financial stability mandates, have discussed potential caps or other limitations on the use of rCBDC.[19] Such restrictions may impose a restrictive upper bound on liquidity in one or more currencies, hindering the FX providers from providing adequate FX services. Likewise, there may be a cost of holding rCBDC vis-à-vis holding reserves or commercial bank money, which could discourage FX providers from holding a sufficient inventory of rCBDC. These potential effects should not be overstated. Monetary policy reconciliation only occurs for a short period in the evening. The central bank could regard rCBDC held by financial institutions as reserves, eliminating the opportunity cost vis-à-vis reserves, and exempt them from any prospective limits.[20]

Most of the potential problems discussed above could be mitigated if central banks were to provide facilities that would enable RTGS participants to instantly access rCBDC against reserves or eligible collateral 24/7. The FX provider would not need to hold rCBDC for a long period of time. The FX provider could even automate the conversion back and forth between rCBDC reserves, traditional reserves, or commercial bank money, thus enabling it to maintain the desired liquidity level without human intervention.

---

19 As an example, see BIS et al (2022b).

20 Some central banks compensate private cash depot owners for forgone interest on all or some of the banknotes and coins held in the depot, partly to reduce the opportunity cost of holding them in the depots. A similar logic could possibly be applied to rCBDC so that FX providers who are also monetary counterparts receive interest rate compensation for amounts held in dedicated FX wallets.

Central banks may even consider expanding the participation of FX providers by allowing non-financial entities who have wallets in more than one rCBDC to serve as FX providers, thereby adding liquidity and increasing competition.

6.5 Pricing of services

In the real world, pricing of cross-border services is important. Payment markets are two-sided, such that the use of a service on one side of the market affects the value of the service on the other side. Private wallet providers in this project do not internalise such network effects in their pricing decisions and may price services too high from a social perspective. In the case of this project, if a payer's wallet provider charges a high fee for supporting a cross-border payment, then the payer may refrain from using it. This reduces the value for the payee abroad in signing up to a cross-border service since they know the payer will not use it. Network size and usage may be less than socially optimal.

In the presence of externalities, such as the network effects discussed earlier, some price regulation or subsidy may be required if the social benefits are to exceed the social costs.[21]

6.6 Privacy and AML/CFT

In this project, the responsibility for KYC, AML/CFT and other due diligence requirements is assumed to lie solely with the wallet providers and a full regulatory analysis has not been undertaken. Besides the information from the KYC process, wallet providers would depend on the information they can extract from the payment messages for compliance. The Icebreaker hub only routes messages and maintains a log, all actors involved in the payment would, over the payment cycle, have access to all relevant information contained in the payment messages.[22] Privacy and competition concerns would need to be properly addressed in the arrangement, and may reflect a trade-off and careful calibration as to how much, and what, information to include in the payment messages so that they conform to applicable data protection regimes and other compliance requirements. Future research could incorporate more innovative technologies for data obfuscation or privacy-enhancing technologies, which would allow the full benefits of the Icebreaker model to be realised while raising fewer privacy concerns.

One key challenge for PSPs in general is they may not have access to all the information needed when conducting compliance.[23] As an example, a wallet

---

21 Card schemes use interchange fees and "honour all cards" rules to address incentive problems related to network effects. This is not without drawbacks, and such fees and rules have attracted the attention of regulators and legislators, resulting in eg the EU's Interchange Fee Regulation.

22 See Appendix B for an overview of the payment message information.

23 The identity of criminals and the origin of funds may be concealed through complicated cross-border structures where illicit funds are transferred between different countries and legal/natural persons. Therefore, financial institutions tend not to have the overview required to identify and report cases of this level of complexity. This is partly the result of laws on bank secrecy and privacy protection.

provider in one country may not know the origin of the funds sent by the payer in another country in a chain of cross-border payments. The hub, on the other hand, presides over a complete log of routed messages and may therefore be able to provide services based on a larger information set, thus facilitating the compliance activities of the wallet providers.[24] The owner of a hub may carefully consider the opportunities to apply new technology and provide services that facilitate and improve the participating institution's ability to carry out their compliance.

6.7 Addressing and payment initiation

The format of the payment message, the information that needs to be included, and the order in which the different steps are taken are predetermined. While outside the scope of Project Icebreaker, it is important to highlight the need for coordination and harmonisation regarding payment initiation. For example, how does someone in one country get the wallet address of someone in another country? In the Icebreaker model, one rCBDC system may use an address system that is very different to that of another rCBDC system. To facilitate easy cross-border payment initiation, a common address standard would be helpful, as would one or several alias databases.[25] The W3C decentralised identifiers (DID) could be useful for addressing and could be an area of further work.

The second issue is how the payer should enter the payment information into its wallet. For card payments at the point of sale, a card terminal communicates with the card, while some mobile payments are done by that wallet scanning a QR code etc. Likewise, each rCBDC system could support multiple such mechanisms. Standardising them would facilitate cross-border CBDC payments.

7. Concluding discussion

The validation of the Icebreaker model shows that central banks have almost full autonomy when designing their domestic rCBDC system. They can opt to use different technology solutions, while still being able to participate in a formalised interlinking arrangement.

The project demonstrates the following benefits:

- It enables cross-border interoperability, allowing systems with different technologies to talk to each other in a standardised way.

[24] The BIS Innovation Hub's Nordic Centre has launched Project Aurora to look at the components of a new data architecture, and ultimately how privacy-enhancing technologies, artificial intelligence and network analytics can be used on centralised payments data to better identify money laundering, terrorist financing, illicit finance, fraud, or systemic risks, both within and across borders. See www.bis.org/about/bisih/locations/se.

[25] Addressing has been studied in Nexus, see BIS Innovation Hub (2021). There is an international standard for bank account numbers (IBAN). rCBDC cross-border payments would be greatly facilitated by something similar for rCBDC.

- It reduces settlement and counterparty risk by the use of coordinated payments in central bank money.
- It allows increased competition and choice for consumers, by decoupling the provision of an FX service from the FX transaction, as well as through the use of bridge currencies.
- It helps reduce costs.
- It helps achieve increased cross-border reach.
- It is scalable, easily connecting the systems of many countries.
- It is fast; transactions take just seconds to complete.
- An rCBDC does not need to leave its rCBDC system.

The minimum technical requirements are:

- The rCBDC system must be able to implement HTLC-based conditional settlement.

- The rCBDC system must operate in real time, or near real time, 24/7/365 to maximise speed and minimise failed payments due to timeout in settlement and message response.

Some key recommendations to a central bank considering implementing a rCBDC system are to:

- Consider ways to incorporate conditional settlement, eg HTLC.

- Consider ways to ensure system availability and short response times 24/7/365 to maximise speed and minimise failed payments.

- Consider adopting current messaging and addressing standards, supporting development of them where they are needed and don't yet exist and ensure flexibility in adopting future standards.

- Consider ways to provide instant rCBDC liquidity provision for FX providers 24/7/365.

- Promote transparent and competitive incentives for FX providers.

For the Icebreaker model, two main considerations could be explored further:

Stateful hub: An alternative design that was investigated but not implemented in the project, envisioned a more active role of the hub in interpreting payment messages and sending partial payment instruction details to the participating wallets.

Alternatives to HTLC: The project did not investigate alternatives to HTLC but this could be considered. The potential for the coexistence of different mechanisms for coordinated settlement deserves further investigation and how this could be implemented in different technical solutions.

Implementing the Icebreaker model in the real world would require a range of technology, policy, and legal considerations to be addressed. Policy considerations include governance arrangements, the viability of the business model, liquidity provision, privacy, AML/CFT, and payment initiation-related standards. Legal considerations would include a sound legal basis for the Icebreaker hub, the potential conflict of laws and regulation between connected rCBDC systems, and conflict resolution. Technical considerations include resilience arrangements and requirements for the Icebreaker hub and participants in the rCBDC systems. Central banks should factor such cross-border aspects into the design of their rCBDC systems to avoid creating unintended barriers for cross-border functionality. The Icebreaker model could serve as a platform for introducing payments innovations (such as delivery versus payment and programmable money use cases) that countries could consider in the context of developing the cross-border capabilities of their CBDC systems.

References

BIS, Bank of Canada, Bank of England, Board of Governors of the Federal Reserve System, European Central Bank, Bank of Japan, Sveriges Riksbank and Swiss National Bank (2020): *Central bank digital currencies: foundational principles and core features*, October.

——— (2021a): *Central bank digital currencies: system design and interoperability*, September.

——— (2021b): *Central bank digital currencies: financial stability implications*, September.

Bank of Israel (2022): *Digital shekel – technological experiment on a distributed platform*, June.

BIS Innovation Hub (2021): *Nexus – A blueprint for instant cross-border payments*, July.

——— (2022): *Using CBDCs across borders: lessons from practical experiments*, June.

BIS Innovation Hub, Hong Kong Monetary Authority, Bank of Thailand, Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates (2022a): *Project mBridge – Connecting economies through CBDC*, October.

BIS Innovation Hub, Central Bank of Malaysia, Monetary Authority of Singapore, Reserve Bank of Australia, and South Africa Reserve Bank (2022b): *Project Dunbar – International settlements using multi-CBDCs*, March.

Committee on Payments and Market Infrastructures (2023): *ISO 20022 harmonisation requirements for enhancing cross-border payments*, Consultative report, March.

Committee on Payments and Market Infrastructures and Technical Committee of the International Organization of Securities Commissions (2012): *Principles for financial market infrastructures*, April.

Committee on Payments and Market Infrastructures (CPMI), BIS Innovation Hub, International Monetary Fund and World Bank Group (2022): *Options for access to and interoperability of CBDCs for cross-border payments*, Report to the G20, July

——— (2023): *Exploring multilateral platforms for cross-border payments*, January.

Kosse, A and I Mattei (2022): "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", *BIS Papers*, no 125, May.

Norges Bank (2021): *Central bank digital currencies – Third report of working group*, Norges Bank Papers, no 1/2021.

Sveriges Riksbank (2021): *E-krona pilot phase 1*, April.

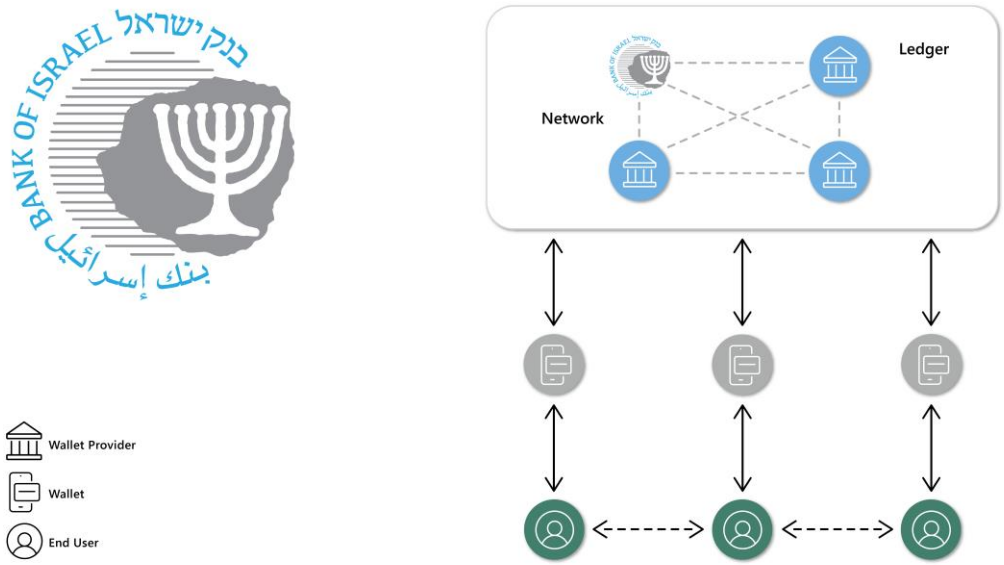
Appendix A: Description of the three PoC rCBDCs

The design of the three PoC systems have similarities and differences, with the common denominator being that they were built for the purpose of conducting a range of different experiments. None of them should be considered as indicative of anyfuture CBDC design decisions of the respective central bank.

Bank of Israel – the digital shekel prototype[26]

The digital shekel experimental environment realises a two-tier model (Graph A1). In this model, although the digital shekel represents a liability of the central bank to the holders of the currency, the end users do not directly approach the central bank to receive, redeem or pay with digital shekels. Their access is via payment service providers (PSPs), which may be banks, other financial institutions or even non-financial entities – a concept that is being examined in Project Sela in order to enable a wider participation of PSPs.[27]

Graph 5. An overview of the ILS-CBDC prototype



[26] For more on the digital shekel, see Bank of Israel (2022).

[27] The BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority and the Bank of Israel joint project to test a cyber-secure retail CBDC architecture that reduces the financial exposure of intermediaries.

CBDC platform – based on DLT

The Bank of Israel established a DLT infrastructure on the Microsoft Azure cloud using Azure Blockchain Services, which enables the realisation of an Ethereum-based Quorum blockchain. The experimental environment included the establishment of a private network, in which four nodes were set up on the blockchain, simulating a situation in which the digital shekel ecosystem includes, other than the central bank, three payment service providers. Each payment service provider is created in a separate node, and the network is fully distributed. The Bank of Israel is the network administrator and defines the payment service providers as validators.

Validation of tokens

The Bank of Israel is the party realising the smart contract that defines the digital currency, and is the sole party authorised to mint or burn coins. The PSPs provide end customers with digital wallet infrastructure and service, through which the customers access the digital shekel network, and it is the PSPs that transfer payment orders between end customers.

Once the system was established, the Bank of Israel "issued" the "digital shekels" using the ERC20 standard. The standard includes currency issuance and payment operations by end users or payment service providers. The use of the ERC20 standard on a standard Ethereum Quorum blockchain basically makes it possible to hold digital shekels issued in the experiment in any standard digital wallet.

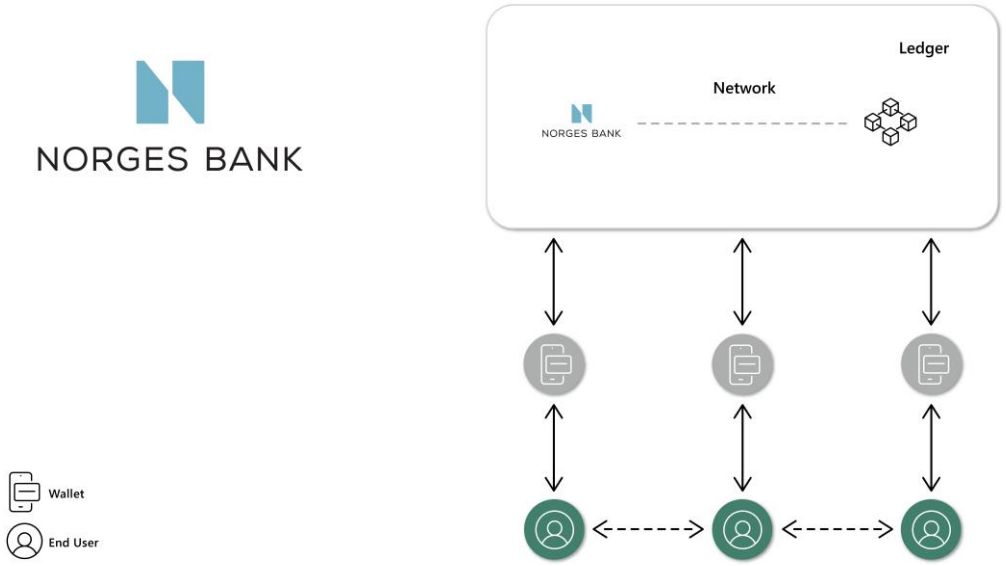
Norges Bank – the NOK-CBDC prototype[28]

The PoC does not constitute a complete payment infrastructure or system. It consists of one core ledger that can be accessed through a non-custodial wallet held by the end user. Both the ledger and the wallet are common for all users, but some users may have special privileges in the system. One example is that only Norges Bank's wallet is allowed to issue and redeem CBDC.

The underlying assumption of the design is that private entities would provide CBDC wallets to the public and that the CBDC would be distributed through the private sector. This functionality is not part of the current test PoC.

[28] Norges Bank has not published the report on the digital NOK-CBDC prototype at the time of the publication of this report. For more on Norges Bank work on CBDC, see Norges Bank (2021).

Graph 6. An overview of the NOK-CBDC prototype



Underlying technology – Hyperledger Besu

The prototype is built in Hyperledger Besu, which is based on the Ethereum network. This includes the Ethereum Virtual Machine (EVM) and, as such, it enables the execution of smart contracts. The test network is private. A central operator decides on admission to the network. The test network consists of several validating nodes and nodes that process smart contracts. The nodes are centrally operated by Norges Bank according to a proof-of-authority consensus mechanism. Money is represented as tokens and the token balances are stored in accounts in a blockchain database. The tokens follow the ERC 20 standard and can contain executable program code. The smart contract at the core of the token cannot be changed by anyone other than the central bank. But smart contract(s) can be built on top of the core smart contract. The design allows for experiments with smart contracts, wallet functionality and interoperability with other networks and ledgers.

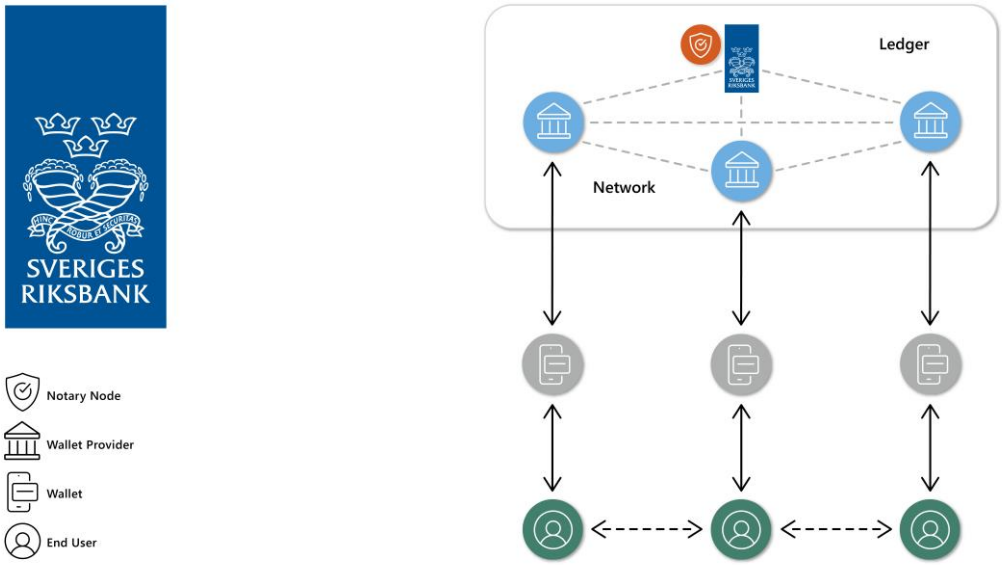
Validation of tokens, settlement, and finality

The wallet is used to initiate transfer tokens between accounts on the blockchain/ledger and to activate smart contracts. Transaction requests are sent from the wallet to the nodes in the network. The nodes are responsible for validating the transactions by checking their signatures and that funds are sufficient for the transactions. The nodes hold the ledger and add new blocks of transactions to the ledger every five seconds.

Sveriges Riksbank – the e-krona test prototype[29]

The design of the e-krona network is based on a two-tier model with the aim of mimicking how physical cash is distributed to the public today. Just as with physical cash, the e-krona is issued and guaranteed by Sveriges Riksbank but it is distributed to the end users via private actors such as banks or payment service providers. The e-krona network is a private network where the Riksbank, as the owner of the e-krona network, must approve those who want to join the network and buy e-krona from the Riksbank and distribute it to their customers. The approved participants manage the onboarding process to the e-krona for their customers, they manage their customers' e-krona wallets and enable transactions, and they design the e-krona services and interfaces on payment instruments for their customers. The conceptual idea of the design is to maintain the Riksbank's role as the creator of money and those of the approved participants as distributors and suppliers to the end users. An illustration of the e-krona network is shown in Graph 6.

Graph 7. An overview of the E-krona prototype



Note: The notary node run by the Riksbank checks for double spending, resulting in finality.

CBDC-platform – based on DLT and UTXO

The e-krona network is based on the Corda DLT platform, which uses a UTXO (unspent transaction output) model. The e-krona is carried by tokens (states), which are immutable records on a ledger that is distributed among its participants. The tokens can be used as input in a transaction (given that the rightful owner of the

[29] For more on the e-krona, see Sveriges Riksbank (2021).

token signs the transaction), which will mark the specific token as spent and create a new output token of e-krona for the payee and a possible token carrying the change for the payer. Thus, each transaction will create a new state on the distributed ledger with a historical reference to the input that created it. Only unspent tokens can be used in a transaction and all unspent e-krona tokens have a transaction chain leading back to the creation of the e-krona at the Riksbank as the sole issuer. The ledger is shared between the participant nodes in the network. The ledger with the historical transactions is, however, not fully distributed between all participants in the network as with some public distributed ledgers. Only the nodes that are directly involved in a transaction will share the new updated information of the states.

Validation of tokens, settlement and finality

The nodes involved in a transaction will also do the validation to check that the e-krona is legitimate and has a historical chain that leads back to the issuance from the Riksbank. This validation will be done by the participant's nodes that are carrying out transactions on behalf of its customers. To fully check that a transaction is valid, the network must also check that the tokens used in a transaction have not been used before, in so-called double-spending. That check is carried out by the notary node run by the Riksbank for the sole purpose of checking that the tokens are unspent. The information of the token's owner (the public key), the payee, the amount etc in a given transaction will not be available for the notary node.[30] The double-spending check done by the notary node represents the finality of a transaction, which means that it is booked on the ledger and cannot be reversed.

[30] The Riksbank will however get the pseudonymised information in the historical backchain when the e-krona are redeemed for destruction back at the Riksbank node.

Appendix B: Payment data in Icebreaker

This appendix describes the data items in the messages routed via the Icebreaker hub (Table B1) and when they are visible to the different actors during the different stages of the payment process in the Icebreaker experiment (Table B2).

Table B1. Data items in the payment messages

Category	Data item	ID
Quote information	FX rate, Bid/Ask, and FX name	1
Amounts in:	Source and target currencies	2
Wallet addresses of:	Payer	3
	Payee	4
	FXP paying "leg" (legs in PvPvP)	5
	FXP receiving "leg" (legs in PvPvP)	6
Wallet providers' hosts of:	Payer	7
	Payee	8
	FXP paying "leg" (legs in PvPvP)	9
	FXP receiving "leg" (legs in PvPvP)	10
Additional monitoring items	Quote ID	11
	Payment ID	12
HTLC information	Hash of secret	13
	Lock max duration	14
	Lock time out in payer system	15
	secret	16

Table B2. Information visibility during the payment process

API	Get quote	Payment discovery	Payment set-up	Payment completion
Entities exposed to data	Payer, Payer's wallet provider, hub	Payer, Payer's wallet provider, Payee's wallet provider, Payee	All	All
Data item ID	1, 2, 5, 6, 9-11	1-14	1-13	1-13

Note: The design solution of the domestic rCBDC system determines to what extent a central has access to data items in payment messages.

Appendix C: Project participants and acknowledgements

Bank of Israel

Yoav Soffer, Digital Shekel Project Manager

Tomer Mizrahi, CTO and Digital Shekel Technology Lead

Amir Moshe, Digital Shekel Economist

Daniel Skorikov, Senior Cloud Architect

Avia Hollander, Senior Software Developer

Ilan Matityahoo, Senior Software Developer

Nawras Dahleh, Senior Software Developer

Rachel Vashdi, Senior Software Developer

Daniel Mirzakandov (technical consultant)

BIS Innovation Hub

Beju Shah, Nordic Centre Head

Björn Segendorf, Adviser

Daniel Eidan, Adviser and Solution Architect

Darko Micic, Cloud Architect

Grimur Sigurdarson, Adviser

William Zhang, Adviser

Norges Bank

Knut Gulleik Sandal, Director

Peder Østbye, Director of Analysis

Lasse Meholm, Coordinator

Suela Kristiansen, Senior Adviser

Terje Åmås, Special Adviser

Stefano Franz (technical consultant)

Ørjan Monsen (technical consultant)

Sveriges Riksbank

Mithra Sundberg, Head of e-krona division

André Reslow, Advisor

David Lööv, Senior Economist

Micael Lindgren, IT Architect

Katarina Telander (technical consultant)

Alisher Zaitov (technical consultant)

Peter de Rooij (technical consultant)

Miska Petoniemi (technical consultant)

Lili Lehti (technical consultant)

Acknowledgements

Special thank you to Cecilia Skingsley, Ross Leckow, Andrew McCormack, Daniel Eidan, Andreas Adriano, Ben Dyson, Codruta Boar, Dessi Cheytanova, Sigrid Sulcebe, Susanne Bohman, Hachem Hassan, Gabriela Guibourg, Elsa Themner, Monika Johansson, Dilan Ölcer, Michal Sinai Livyatan, Helge Syrstad, Nick Vaughan, Manisha Patel, Paola Di Casola, Lukas Ferdinand Petry, Dinesh Shah, Bjarki Vigfusson, Frederick Cheung, Bernia Lee, Yvonne Tsui for supporting this project.

Bank for International Settlements (BIS)

ISBN: 978-92-9259-638-5 (online)