Logical Architecture for the Digital Shekel System

Bank of Israel

March 2024

The Bank of Israel Steering Committee on the Potential of a Digital Shekel Issuance

Bank of Israel - The Bank of Israel Steering Committee on the Potential of a Digital Shekel Issuance

March 2024

Amir Moshe – Digital Shekel Project

Yoav Soffer – Digital Shekel Project

*We wish to thank our colleagues in the Information Technology Department, the Payment and Settlement Systems Department, and the staff and steering committee of the Digital Shekel Project for their insights and their assistance in the writing and editing of this document.

Table of Contents

Glossary and Abbreviations

End user – Private individuals and organizations (businesses, nonprofit organizations, government agencies, etc.) who can hold a balance in digital shekels and use it to make payments among themselves.

Participant – An organization that plays a role in the digital shekel system and is obligated by its rules. In contrast to a participant according to the Payment Systems Law, a participant in the digital shekel system will not necessarily be able to generate payment orders. This document defines four types of participants: the Bank of Israel, digital shekel payment service providers (DS-PSP), funding institutions (FI) and additional service providers (ASP).

Funding Institution (FI) – Financial entities that manage the public's current accounts outside the digital shekel system and which will enable their customers to convert money in their accounts with them into digital shekels (funding) and in the other direction (defunding). For example: commercial banks, the Postal Bank, credit unions, financial asset service providers, etc. Some of the FIs will also support conversion of cash into digital shekels and the reverse for all end users of the digital shekel.

Retail Central Bank Digital Currency (rCBDC) – A digital currency that is issued by the central bank and is the central bank's direct liability; it is intended for use by the general public ("digital cash").

Two-tier model – An operational model for the rCBDC system according to which the end user's access to the system will be based on connecting with intermediaries who will provide the necessary technological and business envelope for the connection.

Back-end – The system components that are needed by the central bank in order to carry out its functions in the digital shekel system, including the databases that are required for or derived from those activities. In particular, the backend will include a settlement "engine", which will enable the transfer of digital shekels as part of payment activities between two end users.

Digital Shekel Payment Service Provider (DS-PSP) or, in short, Payment Service Provider (PSP) – A main participant in the use of the two-tier model of the digital shekel system. This type of participant will be responsible for providing the technological and business envelope needed in order to connect end users to the digital shekel system (the Know Your Client process, provision and recovery of the means of access to the system, customer service, etc.). Without a connection to the payment provider, an end user will not be able to operate in the digital shekel system.

Additional Services Provider (ASP) – An entity of this type will provide additional optional services to end users, such as: budget management, analysis for businesses, fraud monitoring services, innovative payment apps, etc.

Funding/defunding – Conversion of digital money that is not a liability of the central bank (such as a deposit at a commercial bank or at an entity that manages a payment account for the user) into digital shekels, or conversion of cash into digital shekels. The result of funding is an increase in the end user's digital shekel wallet balance. A defunding action is the reverse of a funding action.

Real Time Gross Settlement (RTGS) – A system for disaggregated, immediate and final settlement for transactions between banks and business entities (such as other clearinghouses) and between customers. In Israel, the RTGS system is referred to as ZAHAV (acronym in Hebrew for Real Time Credits and Transfers) and is operated by the Bank of Israel.

Open Banking – Standardization that makes it possible for third parties to access the financial information of a customer with an account managed elsewhere, or to initiate activities in the customer's account. The access of the third party involves the use of APIs that are externalized by the entity managing the account.

Token – A digital representation of value on a platform that can be programed. A token can be the result of a tokenization process, i.e. a representation of value that already exists in a traditional record system (such as a representation of securities that are already listed for trading in an existing system), or which can be issued directly to a particular platform, such as a digital currency token.

Unspent Transaction Output (UTXO) – A model for token-based settlement. In this model, every transaction is composed of the input of a token or tokens that change status to "spent tokens" and which can no longer be used by the end user. At the same time, an output of tokens is created with the status of "unspent tokens" which are issued to the beneficiary side. If necessary, "unspent tokens" will also be issued back to the payer as change.

Ledger – A record-keeping book or digital database in which all financial transactions are tracked and summarized. It serves as the primary accounting record of a company or entity, ensuring that all credits and debits are accounted for and balanced.

Conditional payment – A payment action whose completion is based on the fulfillment of a particular condition, such as the receipt of a package by post (DvP) or the receipt of payment in a different currency (PvP). There are various technological and business mechanisms for the management of a conditional transaction. Most of them involve a locking-in of a certain balance when making the transaction and its release to the beneficiary if a condition is fulfilled or on the activation of a trigger.

Waterfall – A process in which a digital shekel wallet is automatically defunded if the balance in the wallet exceeds the maximum amount that is allowed to be held in the wallet (as a result of a limit on holdings) or where the balance exceeds a particular threshold defined by the end user. This system minimizes the damage to the user experience since it allows the user to receive payments in his digital shekel wallet even if it raises the balance to beyond the holding limit.

Reverse waterfall – A process in which a digital shekel wallet is automatically funded if the balance in the wallet is insufficient to carry out a transaction or if the balance has dropped below a threshold defined by the end user. This system allows for the execution of payments in amounts that exceed the holding limit, and improves the user experience.

1. Background and Main Conclusions

As in the case of many other central banks which are considering the design and issue of a retail digital central bank currency (rCBDC), the Bank of Israel is considering the introduction of a two-tier model for this purpose (Bank of Israel, 2021). In this model, the access of the end user to the CBDC will be by means of intermediaries in the private sector. This paper discusses the various architectures for operationalizing such a two-tier model.

The architectural implementation of the two-tier model has recently been thoroughly considered by other central banks that are examining the issuance of an rCBDC. For example, the ECB (ECB, 2023) and the Bank of England (BIS, 2023c) have carried out technological trials and have entered into partnerships with the private sector in order to determine feasibility. Project Sela, which was recently completed and in which the Bank of Israel collaborated with the BIS Innovation Hub and the Hong Kong Monetary Authority (HKMA), looked at the adoption of a specific two-tier architecture based on the technology proposed by the project's vendor[1] and the business requirements set down by the project participants (BIS, 2023a).

The examination of alternatives in this paper includes emphasis and clarification of a number of important issues: the type of users in the system; the division of functionality between the participants as part of the full implementation of the solution; the model for distribution of the digital shekels from the central bank to the end user; and the various alternatives for the backend layer or the system's engine which will be created and operated by the Bank of Israel (or someone on its behalf).

The main recommendations:

This document was written as part of the design process of the digital shekel and an appropriate logical architecture for it. Section 8 in this paper presents the main conclusions with regard to several important aspects of the logical architecture of the rCBDC system, and in particular the digital shekel system: 1) The types of participants in the system (apart from the PSPs) – the different types of FIs that will facilitate the conversion of money from the accounts that they manage or from cash into digital shekels. 2) The possibility of including an additional type of participant in the system which will provide optional valued-added services. 3) The use of an indirect distribution model in which the Bank of Israel will distribute digital shekels to the FIs and they in turn will support the distribution to the end users. 4) Principles for administering the backend layer while maintaining a clear distinction between the settlement of transactions and information management. 5) Initial principles for the system's interoperability with existing and future infrastructures.

It should be emphasized that the entire document, particularly its recommendations, is agnostic to whatever extent possible with respect to the realization of the architecture. At this stage of the project, the project team is not looking at the choice between the various technologies (such as, for example, a distributed ledger technology or more traditional database technologies). Nonetheless, the awareness of their existence and the feasibility of one technology or another will naturally have an effect on the way in which the logical architecture is thought about.

[1] The realization of the technology in the project was carried out by the FIS and M10 companies.

2. Assumptions and methodology

2.1 Starting assumptions

The role of the logical architecture for the digital shekel is to support the provision of a full solution to end users in the various transactions and activities involving the digital shekel, based on a number of assumptions and decisions that have been made in the project so far, and which have a significant effect on the characteristics of the selected architectural alternatives.

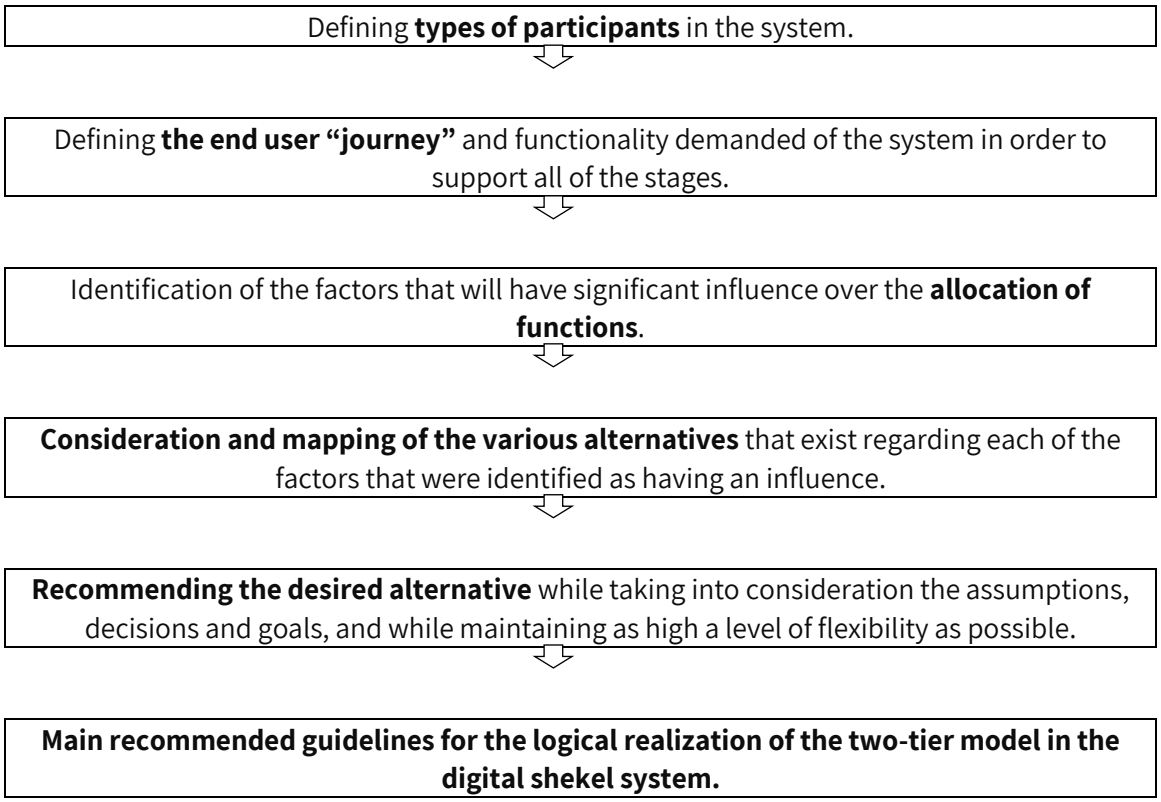
- The architecture will implement the two-tier model;
- The system will support immediate and final payments, 24/7;
- Payment service providers will not create financial exposure as part of the provision of services in the digital shekel framework[2];
- In order to ensure a competitive environment, an end user will be able to operate through multiple payment service providers at any given time;
- The system will support the initiation and enforcement of restrictions, such as limits on the balance that a user can hold in digital shekels;
- The system will support the option for the central bank to have the digital shekel bear interest;
- Interoperability with a solution that allows offline use of the digital shekel will be enabled;
- The architecture will support all design decisions made so far in the project. In particular, in the area of privacy, the architecture will allow the central bank, as the system administrator, to define the types of information required for the operation, control, and monitoring of the system. However, the central bank will not have access to personally identifiable information about end users' balances and transactions. Additionally, the architecture will enable different levels of privacy in the central database according to the type of user (individual, business, etc.), type of transaction, etc.

2.2 Methodology

At the core of the paper is the question of the desired allocation of functions among the various participants, so as to support the full solution required by end users in the system. This allocation will essentially determine how participants will support the execution of different types of actions by users and, of course, it must adhere to the various assumptions mentioned above, as well as striving to achieve the desired business goals of the system. The methodology for identifying the various issues that have a significant impact on the allocation of functions and the logical architecture included several stages (as described in Figure 1).

[2] For further details, see Section 3.2 in the Project Sela Report (BIS, 2023a)

Figure 1 – The various stages in the methodology



The following sections of the paper expand on each of the stages in the above methodology.

3. Types of participants in the system

The digital shekel system will operate as a financial system for immediate payments between end users (individuals, businesses, various organizations, and government agencies). According to the two-tier model, the Bank of Israel and intermediaries will be involved in providing the complete solution to end users. In the layer of intermediaries, a distinction will be made between two types of participants that require different functionality in implementing the solution: payment service providers (PSPs) and funding institutions (FIs). Additionally, there may be additional advanced service providers (ASPs) that end users are not required to interact with, although they will be able to provide end users with additional services, including information services, conditional payments, or other innovative payment applications.

Defining the roles of the various users:

Bank of Israel –Will have exclusive responsibility for the issuance/redemption of digital shekels, and will be entrusted with the administration of the system and its operation (either directly or through an entity appointed by it).

FIs – Funding Institutions are financial bodies that manage current accounts (which are not in digital shekels) for the public (commercial banks, the Postal Bank, credit unions, entities providing financial asset services, etc.), and who will need to enable the conversion of money in the end users' accounts they manage, or conversion of cash, into digital shekels and vice-versa. Different types of FIs can exist, as described in Section 5 of the document and in the following table.[3]

Table 1 – Various configuration of FI activity

Digital shekel holder for the purpose of conversion		**User of another entity's digital shekels[4]**
Directly connected to RTGS	**Represented by another participant in the RTGS**	**C**
A	**B**	

The commercial banks that manage the majority of the public's current accounts will certainly need to act as FIs in Group A in the table. However, the emerging architecture will need to provide flexibility and allow for the existence of the additional models in the table (for example, a nonbank entity represented by a commercial bank in the ZAHAV system).

Payment Service Providers (PSPs) – These entities will be responsible for creating the technological access for end users to the digital shekel system, performing KYC procedures , providing and restoring access to the system, customer service, etc. PSPs will not be financially exposed in their balance sheets at any stage of providing digital shekel services, in accordance with the digital shekel project's working assumption and Project Sela's confirmation of the technological, business, and legal feasibility of this assumption.

There may also be PSPs which are not directly connected to the system and which provide digital shekel services based on connectivity to a payment service provider that is connected to the system (indirect participants).

Additional Advanced Service Providers (ASPs)[5] – These entities will provide additional optional services to end users, such as budget management, business analysis services, fraud monitoring services, etc. In addition, they will be able to take part in bringing together advanced conditional payment services. For

[3] The architectural configurations in the table are theoretical and their business and regulatory feasibility will need to be evaluated.
[4] For example, a user of another FI's digital shekels or on the basis of advanced models that are based on, for example, the end user balances in a liquidity pools mechanism.
[5] The Bank of England refers to a participant of this type as an External Services Interface Provider (ESIP). For further details, see Bank of England (2023).

example, they will be able to act as a third party responsible for sending the "trigger" to lock or release funds in a conditional payment transaction.

These entities will not be able to provide payment services based on direct access to the central bank (as PSPs can). However, it is not impossible that ASPs will be able to provide digital shekel payment initiation services through the PSP chosen by the customer. The definition of this participant's role raises the question of whether it should be allowed direct technological access to the digital shekel's core system at the central bank, or perhaps to limit its access such that it is carried out only through the PSP in a manner similar to that emerging in Open Banking API (for further details on the means of communication between the system participants, see Box 1). Additionally, there is a question regarding the impact of the involvement of this participant on the market's structure (Will there be enough PSPs if it is possible to operate as an ASP? Is there a business model for this type of participant? etc.). Some of the issues relate to policy and regulatory decisions, rather than architectural implementation.

Given that the ASP's access to the core system is limited to specific activities, the initial analysis conducted within the framework of this document raised the possibility that there may be a situation in which the advantages and efficiency of providing it with direct access to the central bank outweigh the negative aspects of the resulting regulatory and technological burden. Therefore, we have chosen at this stage to assume the existence of this participant as part of the architecture, including its direct integration into the core system of the digital shekel, with the goal of ensuring architectural flexibility. However, this assessment will need to be re-examined and tested in the real world in light of the aforementioned business and regulatory questions. In particular, it will need to be understood whether it is possible to achieve the threshold to justify the existence of such a "player", namely a regulatory and technological burden that is less than that of a PSP.

Box 1 – The communication between participants in the digital shekel system

The digital shekel system will need to support the activity of numerous types of entities, and will require two types of communication for proper functioning:

- **Communication between system participants in the private sector and the central bank** – This communication can be implemented through participants' direct access to the API layer, which is externalized by the central bank from the digital shekel platform. (See, for example, BIS, 2023 c). It is reasonable to assume that FIs and PSPs will be given the option to directly communicate with the digital shekel platform. For example, in order to initiate a payment instruction from an end user or to support funding/defunding operations. It is also possible that the activities of these entities will be allowed even without direct connection to the system in a configuration of indirect participants, but this will of course depend on the existence of participants connected directly to the platform.

  Unlike FIs and PSPs, direct communication between an ASP and the central bank is not essential, and ultimately the decision whether to allow direct access will depend on the existing infrastructure in the economy (for example, the existing and developing infrastructure for Open Banking).

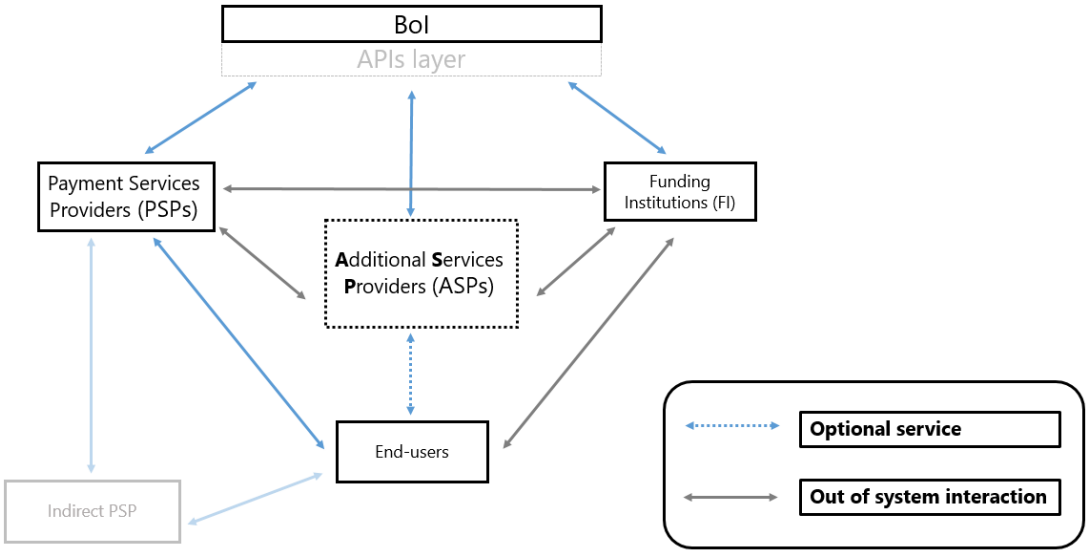
- **Communication between participants** – Communication will also be required between the participants in the system in order to support preliminary operations and/or operations that are complementary to those performed on the digital shekel platform. For example, when an end user requests to fund money from their FI account to their digital shekel wallet managed by a PSP, the PSP will need to check whether the customer has a sufficient balance with the FI in order to carry out the transaction, as well as in the case that it leads to holding a surplus, and the use of a "waterfall" mechanism is required in order to complete it.

Two primary models can be assumed for creating communication between participants:

  - Using the CBDC platform as the link between the participants.
  - Utilizing the existing infrastructure. For example, Open Banking APIs for communication between participants in order to carry out steps that are preliminary to or complementary to the relevant transaction.

Based on considerations of system performance and data security, it is preferable for communication between system participants not to be dependent on the digital shekel platform. Thus, the platform can operate in a "stateless" mode and handle the participant's request after the preliminary communication between the participants has been completed, reducing dependence on complementary processes.

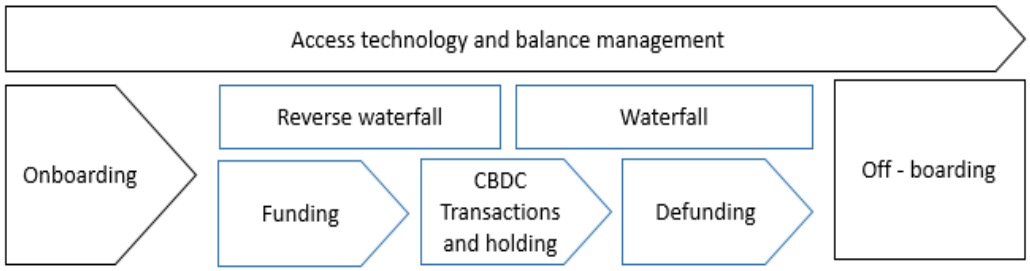
Figure 2 – The participants in providing the solution to the end user in the digital shekel system.



4. The end-user journey and the functionality required of the digital shekel system

The core stages in the user's digital shekel journey, i.e. the everyday use of the digital shekel as a means of payment (in blue in Figure 3), can be distinguished from the supporting stages required to enable the core operations and the completion of the user's journey (in black in Figure 3).

Figure 3 – The end user's digital shekel journey



The logical architecture will need to support the end user's ability to carry out each of the steps presented in the figure.

According to the methodology adopted in this paper, we first mapped the processes that the system must support in order to enable the existence of each stage of the journey:

Figure 4 – The functionality required of the digital shekel system in order to support the user journey (for further details, see Table 2 below):

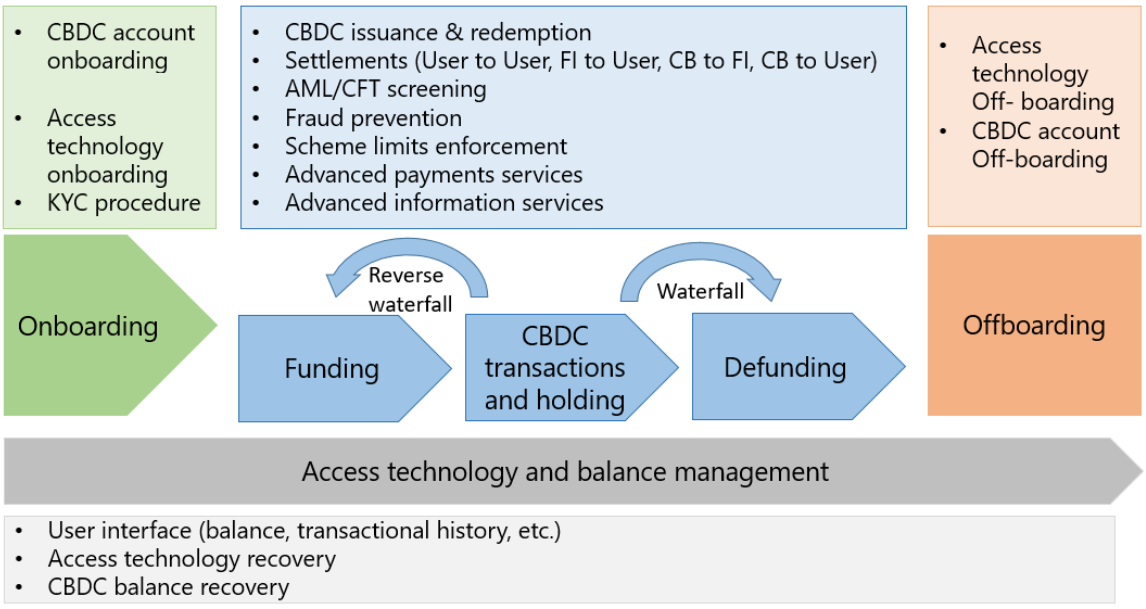


Table 2 – The functionality required of the digital shekel system

Functionality	Explanation
CBDC account onboarding	Connecting the end user to the digital shekel system.
Access technology onboarding	Provision of the technological means that enables access to execute digital shekel operations (smart card, telephone app, POS, etc.)
KYC Procedure	Carrying out the Know Your Customer procedure in the context of an AML/CFT regime.
CBDC Issuance & Redemption	Issuing and redemption of digital shekels by the central bank.
Settlement	Settlement activities of various types: transfer between two end users, transfer between an FI and an end user as part of the funding stage, etc.
AML/CFT screening	A set of actions that the participant will need to perform in order to meet AML/CFT regulatory requirements and system rules.
Fraud prevention	A set of actions that the participant is required to perform in order to meet consumer protection regulatory requirements and system rules.
Scheme limits enforcement	Enforcement of limits, specifically, maximum balance holding limits.
Advanced payments services	Support the end user's ability to carry out advanced payment transactions (conditional payments, periodical payment orders, batch payment, etc.).
Advanced information services	Support the end user's ability to obtain advanced information services: budget management, business analysis, etc.
User interface	Support the end user's ability to manage his digital shekel activity (to view his balance, the history of transactions, etc.).
Access technology recovery	Support the end user's ability to recover the access technology (for example, the loss of a card or the erasure of the cellular device).
CBDC balance recovery	Provide a solution for a situation in which all means of access to the system are unavailable to the end user. For example, a situation in which a particular PSP is no longer active and the system will have to support the end user's ability to connect his balance to a new payment provider.
Access technology offboarding	Abolish the connection of a particular access device to the system.
CBDC account offboarding	Removal of the end user from the digital shekel system, at his request.

Based on mapping all the required functionality of the digital shekel system and identifying the various participants expected to be involved in each function, we concluded that two fundamental architectural issues need to be addressed:[6]

- Distribution model of the digital shekel – How will the digital shekels be distributed from the Bank of Israel to end users? Will this distribution be carried out directly from the central bank to end users, or indirectly, so that the central bank will distribute the digital shekels only to FIs who in turn will distribute them to end users (as in the case of cash distribution)? This issue raises several technological and business questions, which will be discussed in detail in Section 5 below.
- The structure of the backend layer – How will the settlement of digital shekel payment transactions be carried out? And what will be the data structure at the Bank of Israel for this purpose? We have mapped possible configurations for managing the settlement process and the existing data structure at the level of the central bank, while addressing the advantages and disadvantages of each alternative. This topic will be discussed in detail in Section 6 below.

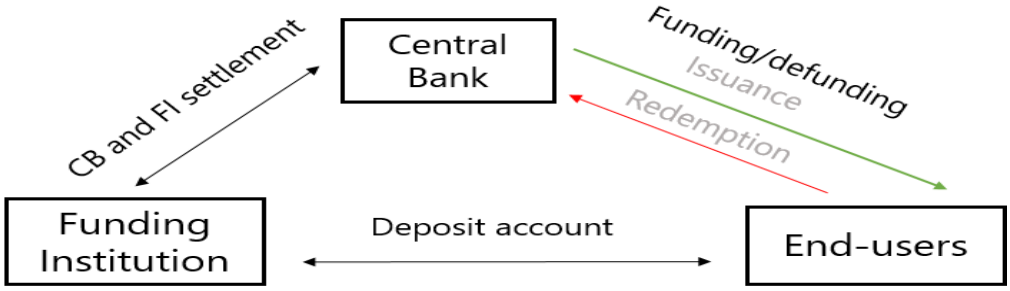
5. The distribution model

We distinguish between two conceptual models for the distribution of digital shekels from the central bank to end users:

- A direct model – The issuance of digital shekels is carried out directly to the accounts of end users. Each request by an end user to perform a funding or defunding[7] operation (against money in an FI account or against cash) will result in the issuance or redemption of digital shekels by the central bank (and simultaneously, an increase or decrease in the FI's reserves at the central bank).[8]

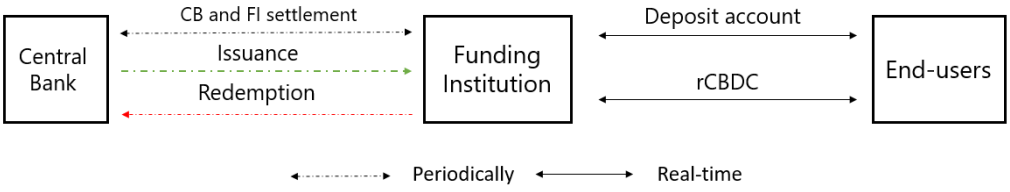
[6] Ignoring the issue of the offline solution which we have decided to relate to, at this stage of the project, as a kind of external component which will require interoperability between it and the system.
[7] Including funding and defunding activities implicit in a payment – Waterfall/Reverse Waterfall.
[8] In the relatively simple situation where the FI has an account at the central bank. There may be a more complex situations in which the FI has an account not at the central bank but rather at a commercial bank (another FI). For further details, see Section 5.3.

Figure 5 –Direct Distribution Model



- An indirect model – The issuance of digital shekels is carried out against the FIs, and the end users' funding and defunding operations increase or decrease the stock of digital shekels held by the FIs to support this operation. In this configuration, the issuance or redemption of digital shekels only occurs when an FI seeks to increase or decrease its stock of digital shekels (as in the case of the existing cash distribution model).

Figure 6 –Indirect Distribution Model



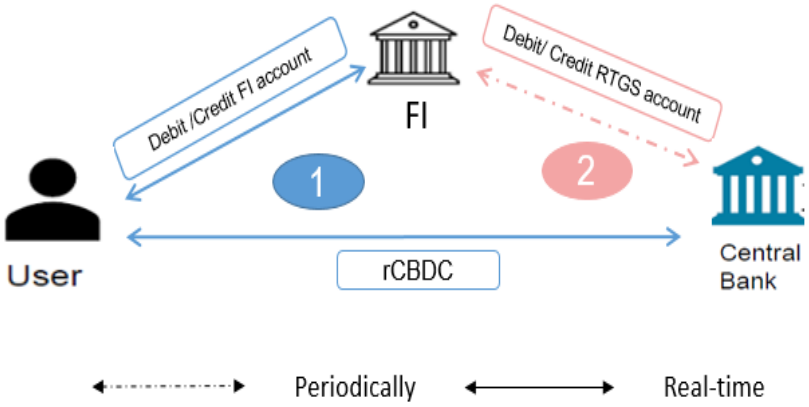
If we could assume that the digital shekel system would be designed to support the technological requirements of direct distribution to end users (issuance/redemption of digital shekels and debiting/crediting against every end user funding/defunding operation, 24/7), then given that in the indirect model, FIs are required to hold a stock of digital shekels at all times (a requirement with potential business implications, particularly with respect to liquidity), it appears that the direct model is more efficient and, in theory, there remains only the question of how to settle accounts between the central bank and the FIs.

However, given that RTGS systems are not available 24/7 and are not suited to support low value-high frequency transactions, **the direct model cannot be implemented by settling accounts between the central bank and the commercial banks on the basis of the RTGS system**. Therefore, based on the architecture examined in Project Sela, alternative solutions for implementing the direct distribution model were considered, while examining the advantages and disadvantages of the proposed solutions in relation to the indirect distribution model.

5.1. Possible solutions for reconciliation between the central and commercial banks in a direct distribution model

- Reconciliation based on net transactions – End users' requests for funding and defunding operations are processed 24/7. However, reconciliation between the central bank and the FI is carried out during settlement windows[9] (similar to the reconciliation process currently in place between commercial banks in Israel based net transactions from the MASAV system).

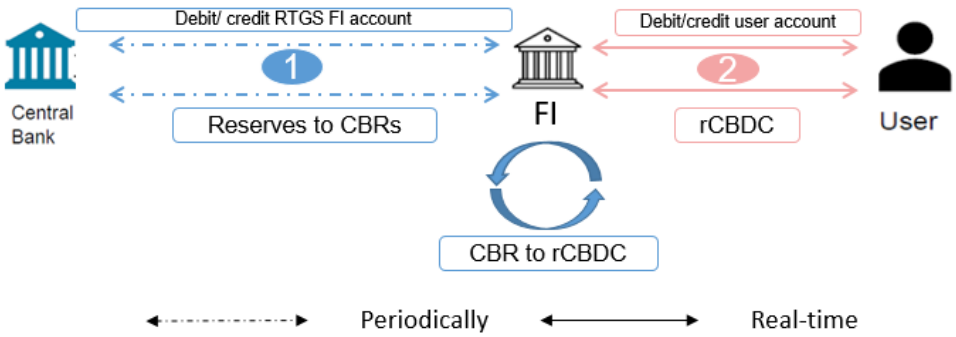
Figure 7 – The net reconciliation solution



- Central Bank Reserves Tokens (CBR Tokens) – This solution makes it possible to overcome the unavailability of the RTGS system based on the following mechanism:
  - FIs can convert reserve surpluses to Central Bank Reserves (CBRs)[10] based on defined settlement windows between the FIs and the central bank, while taking into account the availability of the RTGS system (the bank's reserve balance in CBRs can also be reflected in a "shadow" account in the RTGS);
  - In order to support the funding and defunding operations of end users, FIs will use their CBR surpluses with the central bank, which will redeem CBRs and issue digital shekels directly to end users.

[9] The interval between settlement windows is of course determined by the availability of the RTGS system. For example, it is expected to be longer on weekends and holidays than on regular business days.
[10] Representation by means of tokenization of the banks' reserve balances at the Bank of Israel.

Figure 8 – The CBR tokens solution

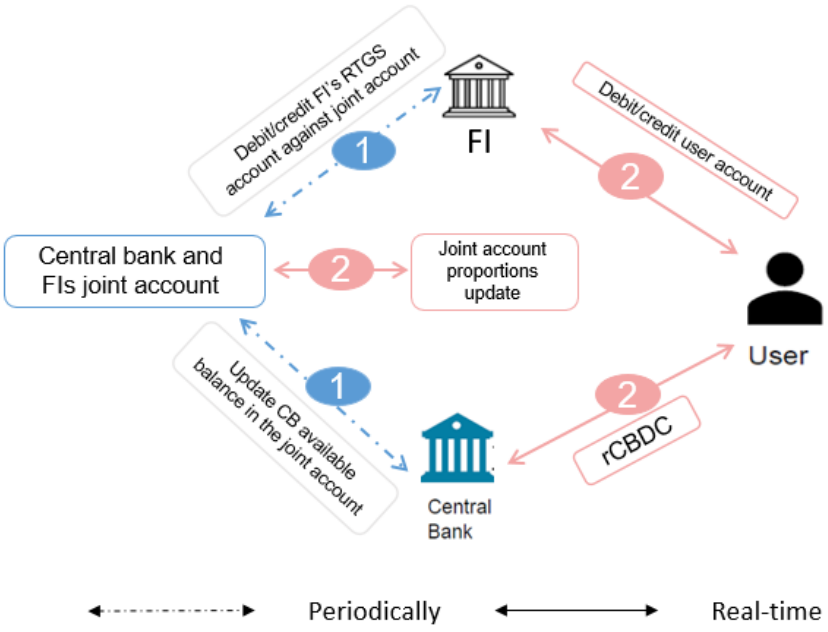


- Real time account to account (A2A)– This solution is based on solutions that already exist in certain jurisdictions to support Fast Payment systems. The system participants share a "common" account and make transfers to it according to the RTGS system's availability. Each transaction between the participants in the system is immediately reflected as a change of the participants' share of holdings in the common account.

  For example, consider a Fast Payment system in which two participant banks each fund the common account with 50 shekels. In the next stage, suppose a user with an account at participant A makes a transfer of 10 shekels to a user with an account at participant B. The implementation of this transaction in the shared account will result in a change in the shares of ownership between the system participants from 50/50 to 60/40 in favor of participant B. Thus, final 24/7 settlement between the system participants becomes possible without being dependent on the availability of the RTGS system.

  The use of this solution for the direct rCBDC distribution model essentially involves managing a "common" account between the central bank and the FIs. Each funding or defunding action by an end user will result in a change in the shares of the common account between the central bank and the FI with which the end user carries out the funding or defunding.

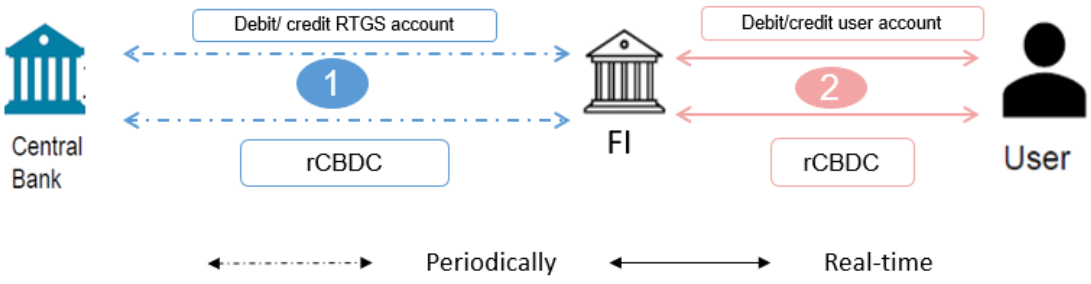
Figure 9 – The A2A real-time solution



5.2 An indirect distribution model

In contrast to solutions for implementing a direct distribution model, in an indirect distribution model FIs acquire digital shekels and hold a stock of CBDC in order to support the funding and defunding operations of end users.

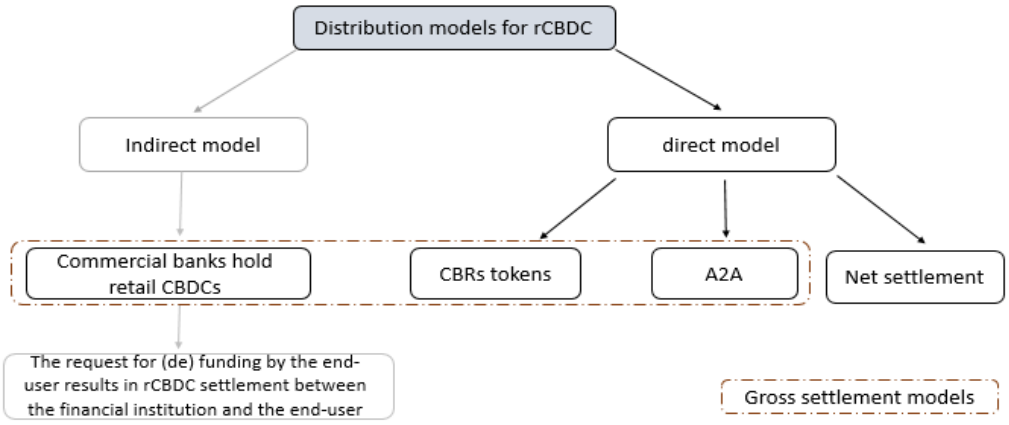
Figure 10 – Possible implementation of an Indirect Distribution Model



5.3. Key considerations in recommending a digital shekel distribution solution

- The net settlement of accounts will result in intraday credit between the central bank and the FIs, and vice-versa. Consequently, only part of the "transaction chain" of the funding/defunding operation will be immediate, since the reconciliation of accounts between the central bank and the FIs is carried out after the fact, based on predefined settlement windows. Furthermore, credit exposure of the central bank to the FI may require the provision of collateral, with all of the resulting complexities and costs.
- A2A and CBRs solutions will require the creation and operation of an additional system, and this will of course have implications for the system's operational and technological complexity. Additionally, managing the reserve balance of the central bank may become more complex due to an additional type of commitment (reserves in the common account/CBRs), in addition to the complexity resulting from the addition of digital shekels to the central bank's balance sheet.
- A2A and CBRs solutions are based on gross settlement and therefore require advance funding of a balance by the FIs in the amount needed to support peaks, rather than based on net transactions. The indirect model is also based on gross settlement (Figure 11).
-

Figure 11 – Mapping the Various Solutions for Implementing rCBDC Distribution Models



When comparing the three models based on gross settlement, consideration should be given to the fact that commercial banks in Israel already have a reserve requirement against the public's current accounts and short-term deposits (of up to a month). This balance does not bear interest and includes the commercial banks' demand deposits at the Bank of Israel and the cash held in their vaults. Digital shekels represent a direct commitment of the central bank and therefore will likely be included in the liquidity buffer. Accordingly, the liquidity/financial impact of the requirement that commercial banks hold digital shekels to support the indirect model is not expected to incur additional costs relative to the other two models.[11]

[11] Apart from an extreme scenario in which all of the non-interest-bearing liquid balance at the central bank is not sufficient to support the funding and defunding activity of end users in addition to everyday activity.

- Moreover, beyond the simplicity of implementation and finality throughout the transaction "chain", the indirect model offers two additional advantages:
    - System performance – As a retail system, the digital shekel system will be required to support high transaction throughput. In order for end users to be able to perform funding and defunding operations at any time, and especially to enable waterfall and reverse waterfall mechanisms, the funding system also needs to support high throughput. In the indirect model, from the perspective of the digital shekel system, a funding or defunding operation is equivalent to a payment operation between the FIs and the end user, i.e. based on the high transaction capability of the payment-supporting system, while in the case of the central bank, the system for issuing and redeeming digital shekels can work in larger batches and therefore with a lower and slower transaction throughput. **Whatever the case, the FIs' systems will need to support frequent updates of their customers' accounts against funding and defunding operations, regardless of the chosen solution**.
    - A step towards a multipurpose currency – The use of a single system by financial institutions and end users can pave the way for a multipurpose digital currency for wholesale and retail use, and will be a step toward solving interoperability issues between the wholesale and retail dimensions.

In summary, the various considerations for choosing one model and solution over another relate to issues associated with the finality of the operation, technological simplicity, and liquidity, which is the most important issue. Taking into account that commercial banks in Israel already need to hold the liquidity requirement that does not bear interest, and which can also include the digital shekel reserves that they will have to hold, **it appears that the indirect distribution model has a clear advantage in funding and defunding operations**.

However, FIs may also operate without directly holding digital shekels (Configuration C in Table 1 above) by, for example, using the digital shekel reserves held by another FI. For example, in a scenario where an e-Money institution holds its customers' funds in deposit with a commercial bank and can support the funding/defunding activity of its customers based on the digital shekel balance held at the commercial bank (for a full description of the distribution operation, see the sequence diagrams in Appendix 2). There may be additional advanced models in which the FI uses a specific amount from its customers' digital shekel balance, known as a Liquidity Pool, based of course on a defined business arrangement between the FI and its customers, and conditional on regulation that allows for this mechanism.

5.4 Funding and defunding against cash[12]

In addition to the ability of end users to fund and defund their digital shekel wallet against an account they manage at a commercial bank or other institution, it is also very important to generate a solution that allows for easy and convenient conversion between digital shekels and cash. If we were content with a solution that allows the end user to convert digital shekels to cash only through the commercial bank where the end user's current account is managed, then the conversion process would be simple and would essentially include two stages:

- Depositing cash in the bank account or withdrawing it based on the existing infrastructure – an action that is not directly related to the digital shekel system, and includes the end user's settlement of accounts with the commercial bank in a manner similar to what is done today;
- Performing a funding/defunding transaction against the customer's account at a commercial bank (as described in detail in the previous section).

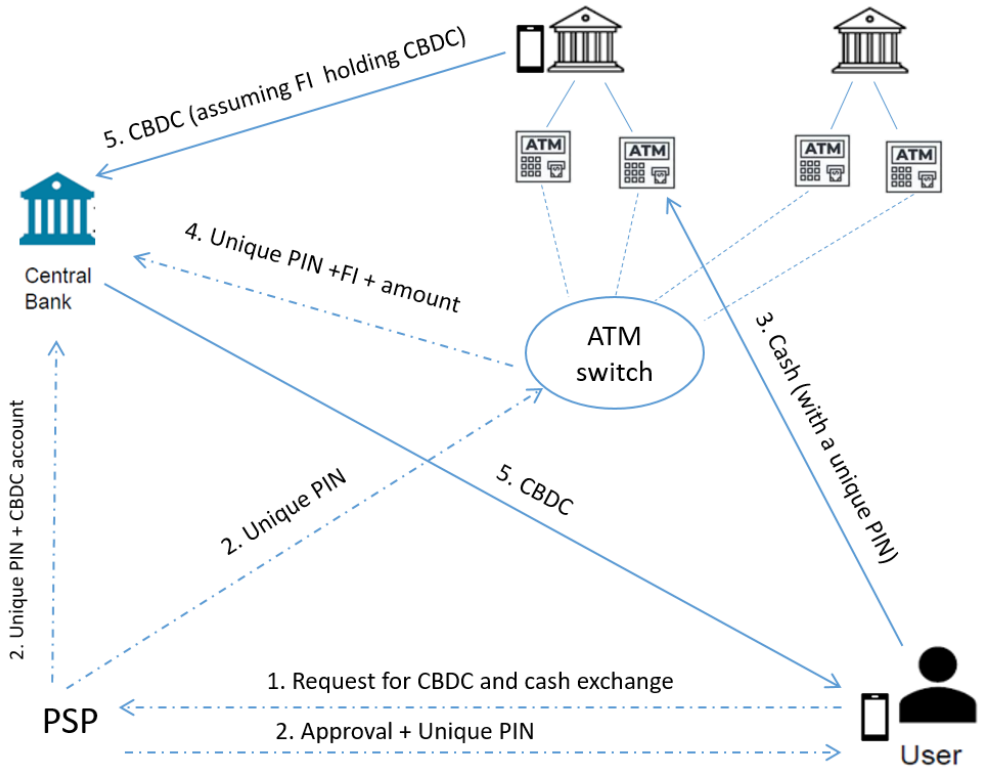
However, **in order to support the conversion operations of digital shekels from/to cash in a more accessible manner, which is not limited to dealing with the financial institution where the end user manages his current account, and also support end users who do not have a bank account, a designated solution would be needed**. A possible configuration is presented below (Figure 12):

- The entities involved in the conversion process: The FIs operating ATMs distributed throughout the country, and the ATMs themselves; the ATM switch; the central bank; the Payment Service Provider (PSP), and the end user.
- The main stages[13] of the solution[14]:
  1. The end user requests (through the digital wallet provided by the PSP) to deposit cash in exchange for digital shekels.
  2. The PSP performs the operational procedures necessary to enable the transaction, including checks required by anti-money laundering regulations. Upon completion of the checks, the PSP sends a confirmation message to the end user, along with a unique code, which is also sent simultaneously to the central bank and the ATM switch.
  3. The end user can access (within a predefined time frame) any ATM in the country that is connected to the ATM switch (and which supports cash deposits) and deposit cash using the unique PIN provided by the PSP.[15]
  4. The ATM switch forwards the necessary details to the central bank in order to complete the transaction: a unique PIN, the FI through which the deposit was made, and the amount. It should be emphasized that there is currently no direct technological connection between the Bank of Israel and the ATM switch, and support for similar processes is not provided. Connectivity and the creation of necessary protocols will be required to support this stage.

[12] Based on the principles of the solution designed in Project Sela.
[13] There may be additional messages between the participants, including confirmation/rejection. Furthermore, the solution presents the "happy path" rather than relating to a scenario of rejection by one of the entities.
[14] For simplicity, a solution is presented for only one direction, namely conversion of cash into digital shekels.
[15] As of now, cash can only be deposited in Israel at the ATM of the bank at which the customer has his account. This may change in the future.

5. Since prior acquaintance or connection between the end user and the FI is not required, the central bank will act as an intermediary between the two entities and will execute the debit operation from the FI's digital shekel wallet and, in parallel, the credit operation to the end user's digital shekel wallet. Since the issuance of digital shekels is performed directly from the central bank to the end user's wallet, **this situation deviates from the indirect distribution model mentioned in the previous section**. Alternatively, the reconciliation can be carried out as a transfer of digital shekels between the FI and the end user, without involving the central bank. However, this configuration might raise privacy and AML compliance issues for the FI.

Figure 12 – A possible process for supporting the system in the conversion of cash to digital shekels and vice versa.



It is possible that the generic solution presented above will enable conversions of low amounts, up to certain thresholds which will be determined on the basis of, among other things, issues related to AML/CFT. For higher amounts, the solution will be based on the two-step process outlined above, requiring deposit to or withdrawal from the end user's bank account.

6. Backend Layer

6.1. Main alternatives for the operation of the settlement "engine"

The Bank of Israel, as the currency issuer and system operator, will act as the responsible and exclusive entity for executing the settlement operation between users and participants in the digital shekel system. There may be two main approaches for the central bank to support this:

- Account-based settlement – According to this approach, the settlement is carried out by updating the balances of end users (debiting the payer and crediting the payee) based on some form of ledger that is capable of linking the user to his balance.[16] This is essentially the traditional approach used in settlement operations today – for example, in bank accounts or in accounts of participants in the RTGS system.
- Token-based clearing – According to this approach, the central bank does not need to know the total balance of the users in order to support the settlement operation, and the operation is based on confirming the authenticity and ownership of a certain balance (represented by a token or a group of tokens). This approach can be viewed as parallel to cash transactions. For instance, to make a payment of NIS 20, the end user can use a 20 shekel note without disclosing the balance in his wallet. It is important to mention that in accordance with decisions made in the project with respect to privacy—according to which the Bank of Israel will not have access to personally identifiable information about end users—the digital shekel will not in fact be anonymous (similar to cash), and the digital shekel system will need to support necessary processes for various regulatory purposes, such as KYC, AML, CFT, tax collection, etc. Therefore, it is reasonable to assume that the total balance of end users will need to be managed in some form of database. However, this is not necessary for the central bank to perform its basic function–the settlement operation.

6.2. Main models for the information structure

There are several possible models through which the settlement mechanism can be implemented, which will be differentiated by, among other things, the structure of the database, the volume of existing data held by the central bank as a default (for the purpose of supporting the settlement operation), and the division of data management between the central bank and the system participants.

The structure of information in account-based settlement

Since settlement operations in an account-based approach are manifested in updating end users' balances, a database in which users (or encrypted identities of users) can be linked to balances is essential. To implement

[16] This does not mean that the connection is made on the basis of the user's identity, and the use of the encrypted identity or any unambiguous identifier that does not enable the identification of the user's identity is feasible.

this approach, there are two conceptual models[17] for data distribution and management between the central bank and the system participants:

- Main retail ledger – End-user balances are managed on the basis of a centralized database at the central bank. It should be emphasized that this does not mean that Distributed Ledger Technology (DLT) cannot be employed in managing the data and its sharing, whether it is managed by the central bank but distributed technologically among various servers of the central bank or managed by the central bank but distributed technologically also among servers belonging to other entities.
- Main wholesale ledger + multiple retail ledgers – In this model, payment providers manage a retail ledger for their customers–the end users–and the aggregate balance of all of a certain payment provider's end users is reflected in the wholesale ledger managed by the central bank. (Here again, it is possible to use DLT technology.)

The structure of information in token-based settlement

In token-based settlement, the central bank is not required to know the end user's total balance, and therefore does not need to accumulate information about the user's activity pattern. However, a centralized database may still be required for other purposes, such as: proper system management, efficiency, maintaining the ability to offer services based on centralized data, managing holding limits, etc. In this model, there is greater flexibility in determining whether to manage a detailed centralized database, and if so, who should manage it, what it should include, and what access permissions the central bank and other participants will have to the data.

As mentioned, there may be many alternatives to the basic data structure. The following are two end possibilities:

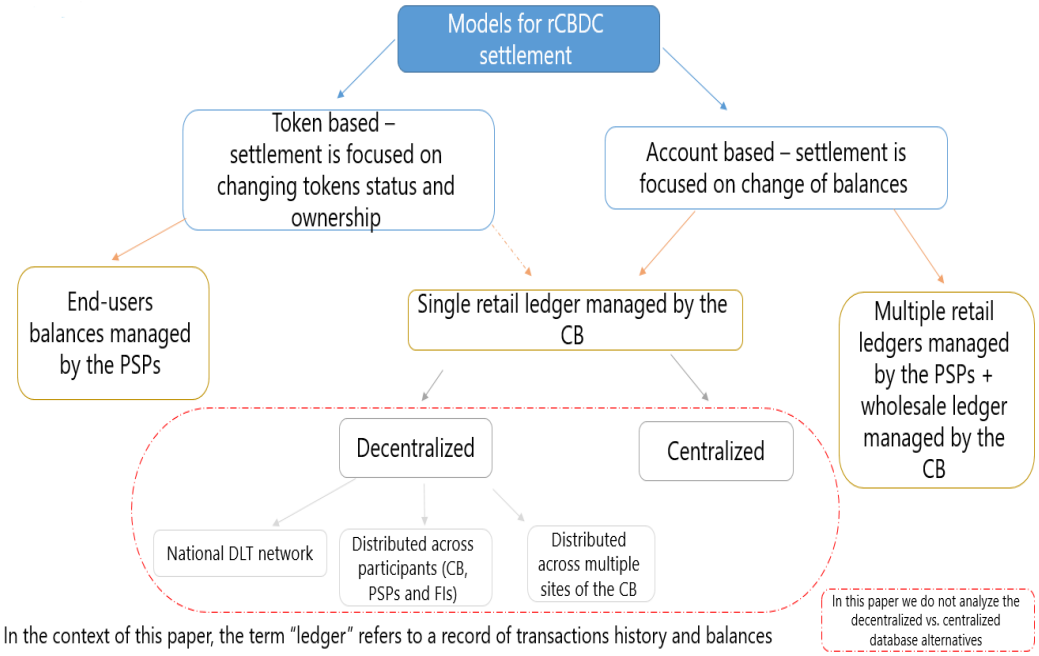
- Minimal information held by the central bank and user balances managed by payment providers[18] – The central database managed by the central bank will include only the information required to support token-based settlement operations such as: tokens available for use and a specific index[19] (such as a public key) which will link the token to its owner. In this model, the management of sensitive and detailed information will be performed solely by payment providers (user identities, total balances, an end user's payment transaction history, etc.), and the central bank will function solely as a settlement "engine." An example of this is UTXO-based settlement (further details appear in Box 2).
- Centralized information similar in scope to that existing in the retail ledger in an account-based approach – Even in a scenario where the central bank decides to handle settlement operations in a token-based approach, it can still be decided to manage a database similar to that existing in the case of a single retail ledger by means of providing a unique index for each end user and storage of the end user's transaction history in the database.

[17] See BIS, 2022.

[18] This model represents the ECB's approach which was presented in the prototyping document (ECB, 2023) and according to which the central bank will operate only as a settlement engine on the basis of the UTXO model, such that user balances will be managed by the payment providers.

[19] This model facilitates a configuration according to which several keys or indexes are connected to one ownership and the central bank does not have to know the ownership (nor the encrypted ownership) of any of the keys in order to carry out settlement.

Figure 13 – The different models for settlement operations and data structure.



6.3. Key considerations in deciding on the data structure model

- Adherence to the preliminary architecture assumptions – The data structure must enable the system to comply with all of the assumptions defined in Section 2.1, including the ability to enforce holding restrictions and to apply interest. In particular, in a case where the interest is dependent on the type of user and/or the size of the balance, there is an advantage to having a centralized database.
- Required functionality – The data structure will need to allow the central bank to support the necessary processes in its role as system administrator, currency issuer, and exclusive entity for carrying out settlement, as well as additional processes in which the central bank may choose to be involved, such as: resolving conflicts between users, supporting the reconstruction of an end user's digital shekel balance (for example, in an emergency situation where a specific PSP ceases to operate), etc.
- Preference for a competitive market structure – The data structure will need to support the end user's ability to receive services from multiple PSPs simultaneously and to easily switch between PSPs, such that the technological and business barriers to entry of participants into the ecosystem will be minimized.

The above analysis suggests that **designing the system in a manner such that the central bank has as detailed a database as possible or a retail ledger** (even if unidentified) **allows for a high level of flexibility regarding each of the aforementioned considerations. On the other hand, managing such a centralized**

database may mean that the central bank will have responsibilities that are typically managed by the private sector, particularly concerning user privacy and enforcement of AML/CFT regulations. In principle, it is desirable for the central bank's involvement in these matters to be as limited as possible. This issue is addressed in the following section, which presents a model with a clear separation between the information required by the central bank for settlement operations and the broader database.

Box 2 – Settlement based on a UTXO (Unspent Transaction Output) model

General Description of the Model:
The UTXO (Unspent Transaction Output) model is a possible application of token-based settlement. Each transaction results in a change in the status of the token or the group of tokens used (the "Input") to the status of "spent tokens," which are no longer available for use, even if their value exceeds the required amount for completing the transaction. The Output of a UTXO transaction includes two or three new groups of tokens:

- A group of tokens previously used as input now has the status of "spent tokens."
- A new group of tokens with the status of "unspent tokens" which is issued to the payee as a single group of tokens with the value of the transaction.
- Optional (depending on the amount of tokens used in the transaction and their value) – a new group of tokens with the status of "unspent tokens" representing the excess issued back to the payer.

In each settlement transaction, the value of spent tokens (Input) = the value of unspent tokens (Output), and users' balances at any given time are calculated by aggregating all of the unspent tokens they own.
Example:
Suppose Bob owns two tokens valued at NIS 50 each, and uses one of them to make a payment of NIS 30 to Alice. The settlement transaction would proceed as follows:

- The NIS 50 token used by Bob is changed to the status of "spent tokens."
- A new "unspent token" worth NIS 20 is issued back to Bob.
- A new "unspent token" worth NIS 30 is issued to Alice.

Bob and Alice's balances after the transaction are calculated based on the aggregation of all the unspent tokens they hold, i.e. NIS 70 for Bob (of which NIS 50 has not yet been spent plus NIS 20 received in the current transaction) and NIS 30 for Alice (received in the current transaction).
Examples of familiar uses of the model:
Many cryptocurrencies, including Bitcoin, rely on the UTXO model for settlement. References to potential use of this model can be found also in the context of rCBDC in projects such as the Swedish e-Krona pilot (Sveriges Riksbank, 2022), BIS's Project Aurum in collaboration with the Monetary Authority of Hong Kong (BIS, 2022), as well as in documents related to the ECB's Digital Euro project (ECB, 2023) and those of the Bank of England (Bank of England, 2023), where the model is mentioned as a possible alternative for implementing settlement engines in the context of account-based settlement.
The information existing in UTXO tokens:
The information contained in each UTXO token consists of 3 fields:

- The value represented by the token ("Value")
- A unique serial number for the token ("Serial number")
- A specific parameter determining who is authorized to use the token and in what manner ("Witness Program Commitment") – The simplest implementation of this

parameter is by using a public key that determines who is authorized to use the token, where usage is only by means of the private key held by the token holder.

Unlike the account-based approach, which allows for a level of pseudonymous privacy of identity at most, the UTXO model allows for greater flexibility and the highest level of privacy, by, for example, using interchangeable "keys" or a number of keys for one user.

6.4 Separating the database from settlement operations – the proposed model

Highlights of the model:

- At this stage of the project, we are attempting not to favor any specific technology and, in particular, we do not want to decide whether the settlement mechanism will be account-based or token-based. The examples presented will assume token-based settlement for purposes of simplicity only, but the proposed model can also be implemented in the case of account-based settlement by using a number of sub-accounts attached to a single "master account". This is similar to a configuration in which tokens are attached to different indexes that are linked to one ownership.
- The basic configuration of the system will support a situation in which the information transferred from the PSPs to the central bank for handling digital shekel transactions will include only the minimal information required by the central bank to execute the settlement. In other words, the public key or any other index associated with the payer's balance/tokens, any unique index associated with the payee, and the transaction amount.[20]
- Characteristics of the central database:
  - Operation and management of the database can be carried out by the central bank, the private sector, or a combination of both. In any case, the central bank will have exclusive authority to make changes to the database (for example, balance adjustments for payment settlement between two users), while the authorizations of participants from the private sector to access the database will be restricted to read-only,[21] according to authorizations granted by end users to participants and in accordance with the system's rulebook.
  - For each user, the structure of the central database will include some encrypted identity (left-hand column in Figure 14) and all the sub-accounts or indexes associated with it (middle column in Figure 14), together with the balance available for use in each sub-account/index (right-hand column in Figure 14). The fact that the balance is divided among multiple indexes does not prevent the end user from using his entire balance through one PSP (including that linked to an index provided by another PSP). This will be possible depending on the system rules and user permissions granted to a specific PSP.

[20] At a later stage, the central bank can decide that for the sake of the system's proper operation or to meet statistical needs, the message received from the payment provider will also include additional characteristics of the transaction or the users and on the condition that they cannot be used to reveal the identity of the users.

[21] In particular, the participants will not be able to change user balances. There may a configuration in which the payment providers will be able to write "smart contracts" in the central database according to the decisions that will be made regarding the use of programmability in the system.

Figure 14 – Example of existing information in the database regarding the user Alice

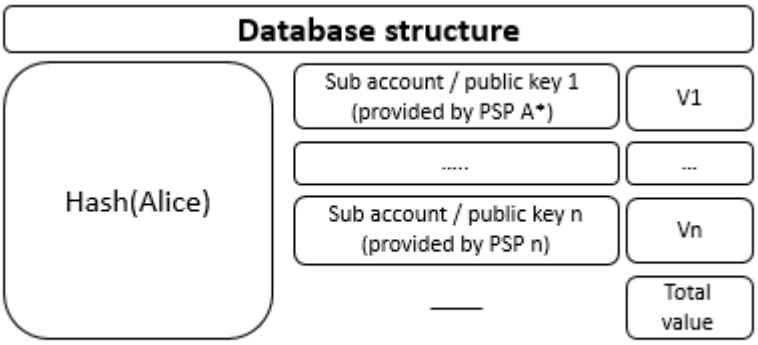
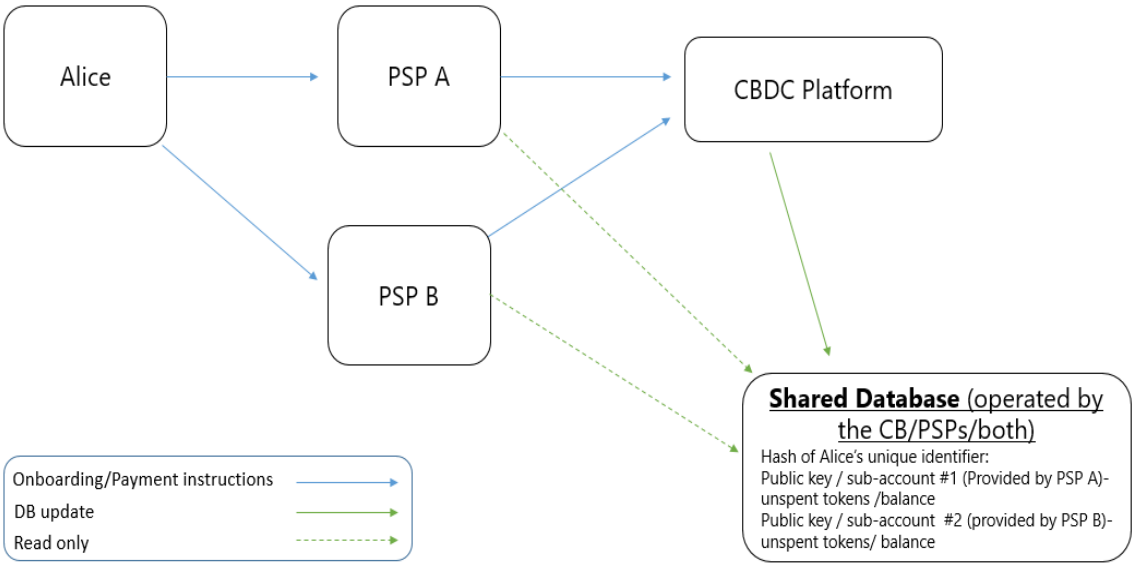


Figure 15 – General structure of the information model.

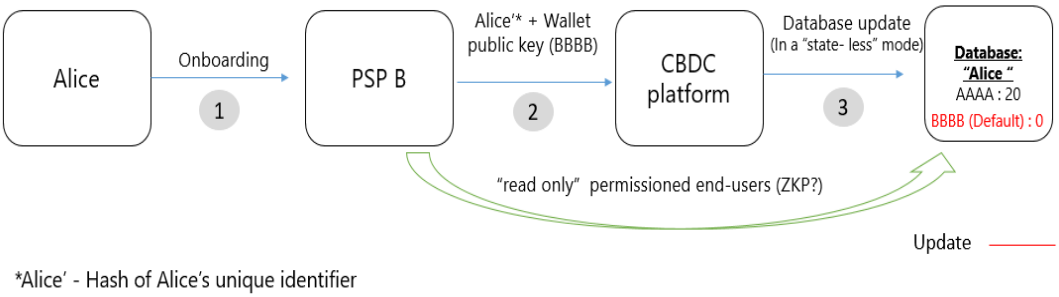


Examples of model implementation:

- Case A – To start with, end user Alice holds 20 digital shekels in a wallet provided by PSP A and she turns to PSP B (Stage 1, Figure 16) since she wants to onboard with them as well, and define B as the default wallet for receiving digital shekel payments.[22] PSP B turns to the digital shekel system (Stage 2) and requests to establish an additional wallet for Alice's encrypted identity (Alice'). The digital shekel system establishes the additional wallet in the database (Stage 3).

[22] While the user can choose the PSP for carrying out any payment transaction, it will likely be necessary to define a PSP as the default in the receipt of payments. In this way, the payer will only need to know the payee's general address without having to know anything else about the various PSPs with which the payee is a customer.

Figure 16 – Onboarding in the proposed model



*Alice' - Hash of Alice's unique identifier

- Case B – Bob is another user in the system and he holds a total of NIS 100 (NIS 50 in a wallet provided by PSP C and another NIS 50 in a wallet provided by PSP D – Figure 17.1). He wants to pay Alice an amount of NIS 30 by means of PSP C (Figure 17.2). He issues the instruction to PSP C (stage 1) which forwards it to the digital shekel system (stage 2). The system verifies that Bob has the required balance and identifies Alice's default account for digital shekel transactions (stage 3), processes the transaction (stage 4), and updates the database regarding the new balances of both users (stage 5).

Figure 17.1 – Database at the starting point in Case B

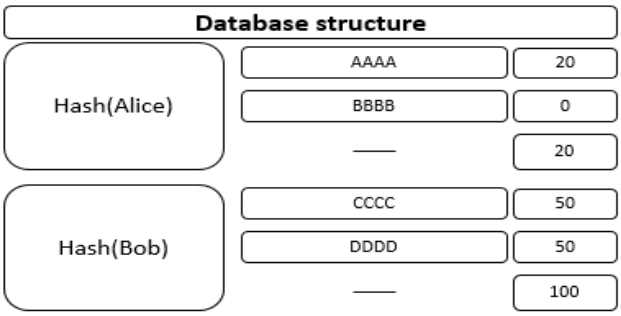
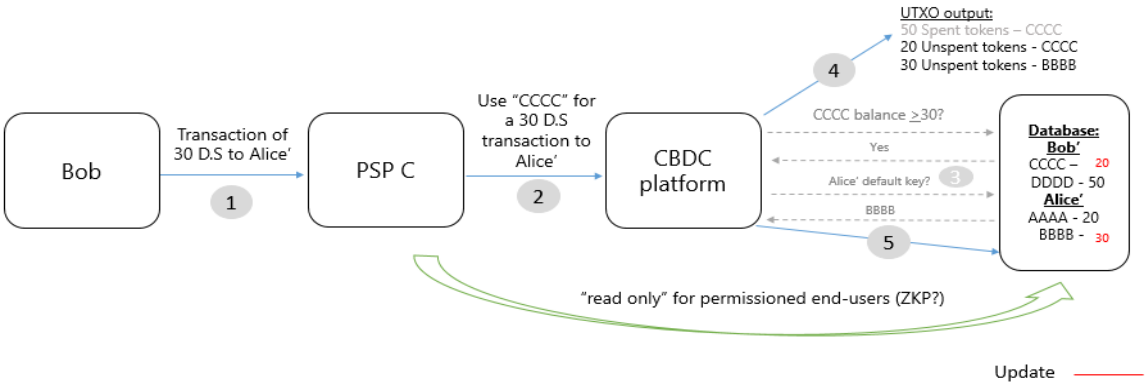


Figure 17.2 – Making the payment from Bob to Alice



6.5 Main advantages of the proposed model

- **High flexibility in implementation**:
  - The proposed model makes it possible, on the one hand, to minimize the information accessible to the central bank to only that required for processing the transaction, while on the other hand providing the flexibility to decide on the characteristics of the database according to additional needs besides transaction processing. The scope of information in the database that is accessible to the central bank can be decided on, as well as the manner in which both the central bank and other participants can access the information in the database.
  - The model can be implemented in both an account-based and token-based settlement approach.
- **Flexible management of the database and access authorizations**
  - If traditional models are used for account-based settlement, it is reasonable to assume that the central database will be operated by the central bank in a centralized manner, since changes in the database essentially constitute a settlement operation, which is the sole responsibility of the central bank. The model proposed in this document offers a more open approach to database management, while distinguishing between the basic information exposed to the central bank regarding settlement operations and the management of the database, even in the case of the account-based approach. Thus, the model allows for greater flexibility in decision making and control over the database. For example, it can be decided that the database will be managed by a distributed network of system participants, a distributed network of system participants and the central bank, etc.
  - Efficient and flexible management of data access authorizations:
    - The access authorizations of the central bank can be decided on, as well as which technology will be used. For example, it is possible to ensure that every entity in the system has access only to the information required by it, by means of advanced "zero-knowledge proof" (ZKP) methods, and to ensure that improper use of information is prevented.
    - Payment service provider (PSP) authorizations to access user balances – Based on the system rules and/or subject to end user authorization, it can be decided whether a specific PSP will be authorized to access and initiate payments even on balances linked to other payment providers. For example, an end user may decide to distribute its digital shekel balance so that each PSP is only authorized to operate on the portion of the balance allocated to it. Conversely, the user may be able to operate through a specific PSP using any balance that he possesses, even if a portion of it is under a sub-account/public key assigned to him by another PSP.[23]
    - Management of separate end user wallets – Separating the user's balance into multiple indices/sub-accounts/private keys allows the end user to split his digital shekel balances into several designated wallets. For example, a certain amount in a wallet that is shared with his spouse. It should be noted that this separation can be based on a number of wallets provided by the same payment provider or by several payment providers.

[23] This option contributes to creating a competitive ecosystem but may be problematic and confusing with respect to the user experience. Whatever the case, the model allows for it.

- **Potential for a positive contribution to system performance**

  Unlike traditional models of account-based settlement, there is no dependency between updating of the end user's total balance and the ability to complete a subsequent settlement transaction for the user. The ability to handle multiple settlement transactions in parallel for a single user (in multiple sub-accounts, for example) has the potential to improve system performance.

7. Other issues

7.1 Interoperability

An important issue in designing the full architecture for the digital shekel system is interoperability with the following:

- Existing systems and infrastructure in the local payments market and in the economy as a whole;
- A system that will allow offline payments;
- Solutions that will be developed for cross-border payments.

A deeper examination of the business and technological aspects of each of these issues will be carried out later in the Digital Shekel Project. This paper refers to them only for the purpose of initial assessment of a full architecture of the digital shekel system, including components and systems for which interoperability is required.

Interoperability is required with existing systems and infrastructure

- The ZAHAV system – Section 5.2 of this paper describes the distribution model, according to which the RTGS system will be used for settlement of accounts between the central bank and the FI against issuance or redemption of digital shekels.[24]
- The ATM switch – For the system to support the generic solution for cash-to-digital shekel conversion (and vice versa) described in Section 5.4 of the paper, connectivity will be required between the digital shekel system and the ATM switch (either directly or by way of the PSPs).
- MASAV (Bank Clearinghouse) – Some of the bank account services provided by MAAV to businesses (such as payroll payment, supplier payments, etc.) can also be provided in digital shekels. A business end user can choose to pay its suppliers or employees using digital shekels rather than from or to a bank account. However, it is possible that some of the services currently offered by MASAV by way of

[24] In the long term, the digital shekel system can serve as the central bank's multi-purpose digital currency, as well as an RTGS system.

bank accounts will be offered in digital shekels by payment providers who will offer advanced services that are not based on MASAV.

- SHVA (Automated Bank Services) – The communication between merchant acquirers and issuers in the credit card system is currently based on the SHVA switch. It can be assumed that communication between payment providers in the digital shekel system will primarily rely on the digital shekel system itself, and possibly also on existing infrastructure such as the existing Open Banking API infrastructure. However, it is not inconceivable that in order to allow end users to make payments at places of business based on existing POS infrastructure that is also connected to the business's cash registers, certain connections will be needed by way of SHVA's existing protocols. Additionally, a configuration may be possible in which an end user chooses that his credit card will debit his digital shekel wallet rather than his bank account.
- Open Banking API infrastructure – Continuous communication is also required between system participants in order to ensure the normal operation of the system (see Box 1 above). The connectivity needed for preliminary and/or complementary actions to those performed on the digital shekel platform can be based on the Open Banking API infrastructure, provided that the infrastructure supports it.

Offline payment solution:

At this stage, it is unclear how an offline payment solution will look in the digital shekel system. However, the impact of the chosen offline solution on the design of the online system is likely to be limited to maintaining a mechanism for conversion from online to offline, and vice versa. Therefore, from an architectural perspective, the offline solution can be viewed at this stage as an external component, which will require interoperability with the system.

Nonetheless, it is worth noting that there are two main conceptual approaches to managing information on offline balances in circulation:

- Assigning an offline balance to each end user – This involves a balance that is known at the time of the most recent connection by the end user to the network. It is reasonable to assume that in most cases, the balances of the users appearing in the database will not accurately represent their exact offline balances, since they will have carried out transactions while not connected to the network, which were therefore not recorded in the database. However, the total offline balances of users will always accurately represent the volume of digital shekels in offline circulation (which only changes in the case of conversion from online to offline or vice versa). This approach can help in managing the risk associated with implementing an offline solution (see Table 3).

Table 3 – An example of assigning offline balances to the end users

End-user	Online balance	Offline balance	Total
A	100	20	120
B	50	30	80
Outstanding CBDC	150	50	200

As of last online update

- Management of all CBDC balances offline as a single entity (similar to cash balance in circulation). In this approach, there will be no information in the database except for the total offline balance. This is similar to the information held by the Bank of Israel regarding the value of cash in circulation (Table 4).

Table 4 – Offline management of balances as a single aggregate

	Online balance	Offline balance
A	100	50
B	50	
Total outstanding	200	

Solutions for Cross-Border Payments in CBDC

On the conceptual level, there are several possible models for achieving benefit in the area of cross-border transfers using rCBDC. For example, using a single platform for multiple countries (i.e. a common platform) or connecting several systems based on a hub-and-spoke system.[25] At this point, there is no clear global direction on how interoperability between rCBDC systems of different countries can be achieved.

7.2 Services based on a centralized database

The existence of a centralized database in the digital shekel system can facilitate higher efficiency in the delivery of certain services. For example, it can support a centralized system which PSPs can use for "know your customer" processes, or for fraud monitoring systems. For such systems, whether operated by the central bank itself, an entity on its behalf, or a technological and regulatory infrastructure that supports private sector participation in these services, there may be business and regulatory implications, such as privacy considerations, the desired level of involvement by the central bank in service provision, the

[25] The model that was used in Project Icebreaker.

contribution of the service to market efficiency, regulatory feasibility, etc. These implications will need to be examined before deciding to establish such a system based on the central database.

7.3 Main issues regarding the frontend layer

While this paper primarily deals with the architecture of the core system, the peripherals that end users will use and the way they will connect to the system are integral parts of the digital shekel system architecture. An access technology will include two main components:

- User interface – This component enables the identification of the end user and makes it possible for him to use the digital shekel.
- Secured container – This component enables the storage of sensitive end-user information, such as his private key or his tokens for offline use. It is the component that facilitates the secure execution of transactions following an instruction given by the end user through the user interface.

8. Conclusions and Recommendations

This document was written as part of the digital shekel design process. As part of the process, the project team analyzes various issues,[26] and the steering committee makes design decisions based on the team's recommendations. Given the interdependence between the various components of the digital shekel system, the decisions are not final. Nonetheless, the decisions will accumulate to form a detailed document and they guide the team's analysis of the various issues. The following are a number of recommendations to be considered based on this paper.

System Participants and Connectivity:

The digital shekel system will support the participation of three types of participants: Digital Shekel Payment Service Providers (DS-PSP),[27] Financial Institutions (FI), and Additional Service Providers (ASP). However, it may be possible for a participant to perform more than one role in the system. For example, an FI can also function as a PSP.

[26] For a list of the topics analyzed as part of the design process, go to: Bank of Israel: Where we stand with the digital shekel project – Yoav Soffer

[27] There may also be a PSP that is an indirect participant. In other words, it will not be directly connected to the system.

- The system will support the participation of various types of FIs, whether or not they are connected to the RTGS system.
- The activity of an ASP participant on the basis of the proposed functionality in the digital shekel system will be limited to a small number of operations, with the goal of minimizing the regulatory and technological burden on such participants within the system.
- The system will be designed in such a way that it strives, as much as possible, to establish the necessary communication between system participants for preliminary or complementary activities to those carried out on the digital shekel platform (checking the balance in an FI account before funding, activating the Waterfall mechanism in case of an operation causing a deviation from the holding limit, etc.) based on the existing (and future) infrastructure for communication between entities in the payment system, such as the Open Banking API. However, if it is found that the existing channels do not allow for the required functionality and efficiency in this communication, alternatives will be considered (improving existing infrastructure and adapting it to the needs of the digital shekel system, communication via the digital shekel platform, etc.).

The distribution model:

- The Bank of Israel will utilize an indirect distribution model for distributing digital shekels to the public, through the FIs.
- The digital shekel system will support a universal solution for converting between cash and digital shekels without relying on the end user's bank account or its existence in general. The thresholds for using this universal solution will need to be determined based on various business and regulatory considerations. Nevertheless, the system will also support conversion based on a two-step process of depositing cash into the end user's bank account or withdrawing cash from it, followed by funding or defunding against the money in the account.

Principles for designing the backend layer:

- The backend layer will be designed with a clear distinction between the settlement engine and the broader database, which the central bank will decide whether and how to manage.
- The system will support a configuration such that as a default the minimum information transferred from the participants to the central bank for operations in digital shekels will be that required for settlement by the central bank.
- The system will also support a possible expansion whereby the central bank can decide that the message received from the PSP will also include additional characteristics of the transaction or the user, as long as these cannot be used to expose the user's identity.
- Characteristics of the central database:
  - The central bank will have the exclusive authority to make changes to the central database, while participants from the private sector will have read-only access, according to end-user authorizations and the system’s rulebook.
  - The structure of the central database will include a unique identifier for each system user, along with all associated sub-accounts or indexes that belong to him, along with the value available for use in each index and in total.

Interoperability and services based on the central database:

- The design of the digital shekel system will take into consideration interoperability with at least the following systems: the ZAHAV system, the ATM switch, MASAV, SHVA and Open Banking API.
- The development of the online solution within the digital shekel system will take into consideration the need of the end user to transition between online and offline balances (according to the offline solution that would be implemented).
- The design of the system will also take into consideration the option of providing certain services on the basis of the centralized database.

Bibliography

Bank of England (2023): "The Digital Pound: A New Form of Money for Households and Businesses?", Consultation Paper, February.

Bank of Israel (2021): "A Bank of Israel Digital Shekel – Potential Benefits, Draft Model, and Issues to Examine." Jerusalem: Bank of Israel.

BIS (2022): "A Prototype for Two-Tier Central Bank Digital Currency (CBDC)", Project Aurum, October.

BIS (2023a): "An Accessible and Secure Retail CBDC Ecosystem", Project Sela, September.

BIS (2023b): "Breaking New Paths in Cross-Border Retail CBDC Payments", Project Icebreaker, March.

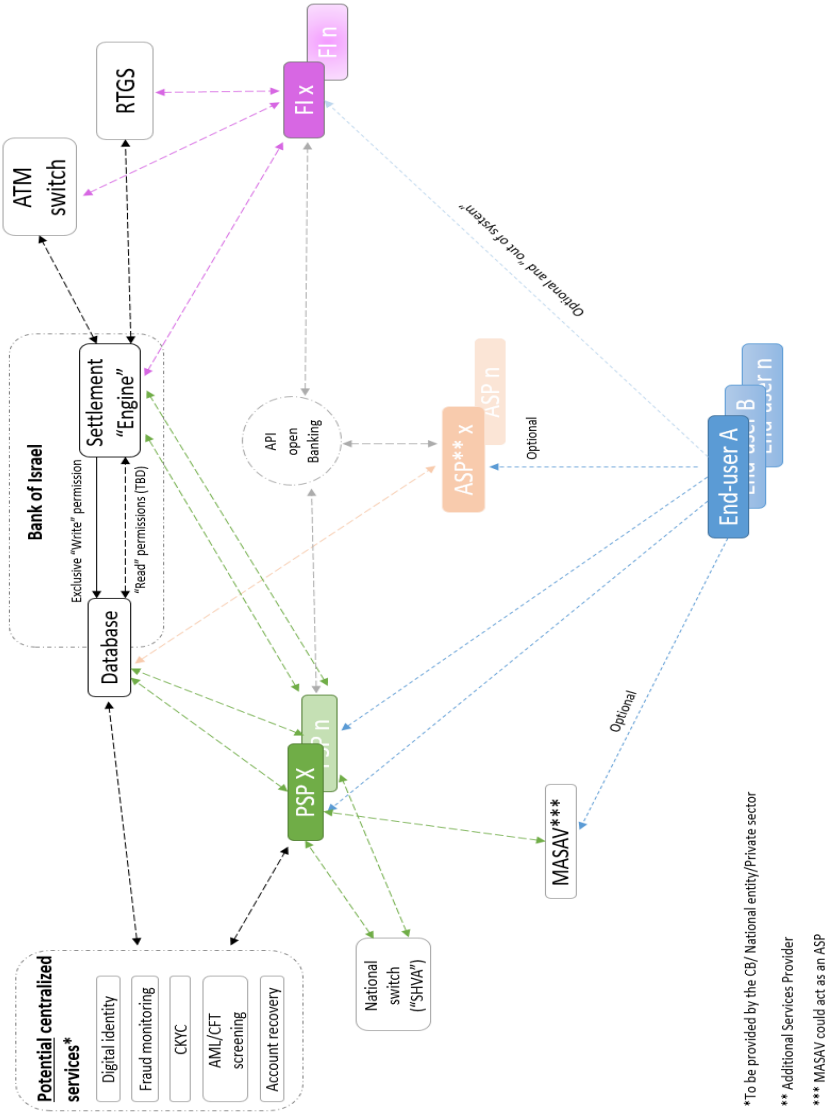
BIS (2023c): "Project Rosalind: Developing Prototypes for an Application Programming Interface to Distribute Retail CBDC", Final report, June.

ECB (2023): "Digital Euro – Prototype Summary and Lessons Learned", May.

Sveriges Riksbank (2022): "E-Krona Pilot – Phase 2", April.

Appendix 1 – A possible configuration for a full logical architecture for the digital shekel system

Figure 18: Full logical architecture



Appendix 2 – Sequence diagrams for the distribution of digital shekels in the indirect model

Figures 19.1 and 19.2 present the sequence of business stages required to support the funding operation of the digital shekel wallet of an end user who is also a customer of an FI which is connected directly to the RTGS system and holds digital shekels (Configuration A in Section 3 above).

Figure 19.1: Purchase of digital shekels by "Bank A"

In the first stage, the FI purchases digital shekels against the balance in its RTGS account:

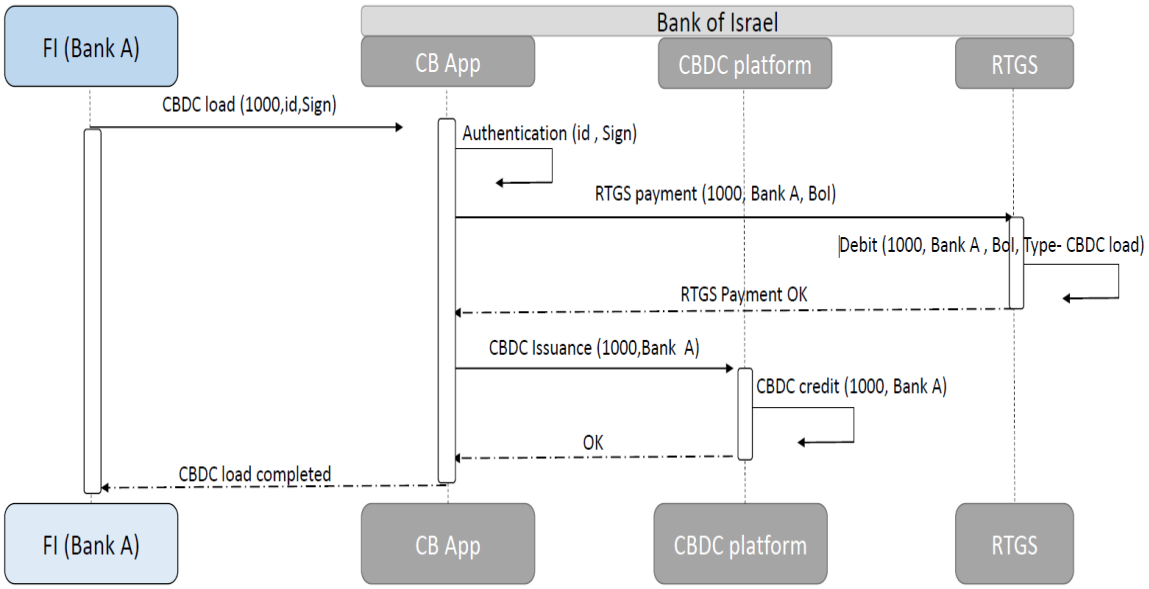


Figure 19.2: Funding of digital shekels by a customer of Bank A.

We now assume that Benny is a customer of PSP A and wishes to fund 100 digital shekels against a debit of his bank account at Bank A (which is connected to the wallet).

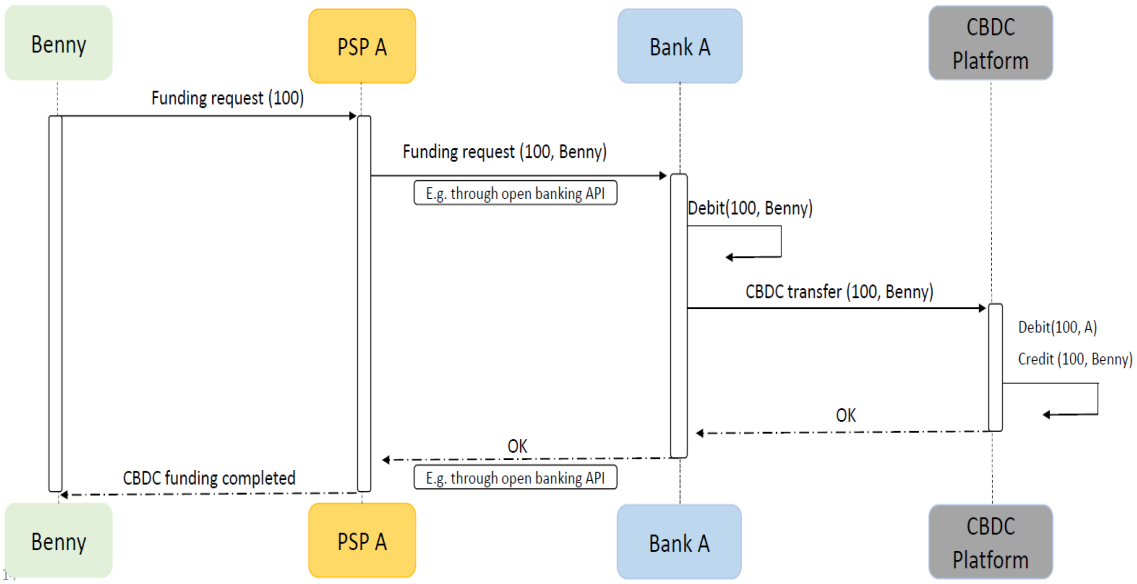
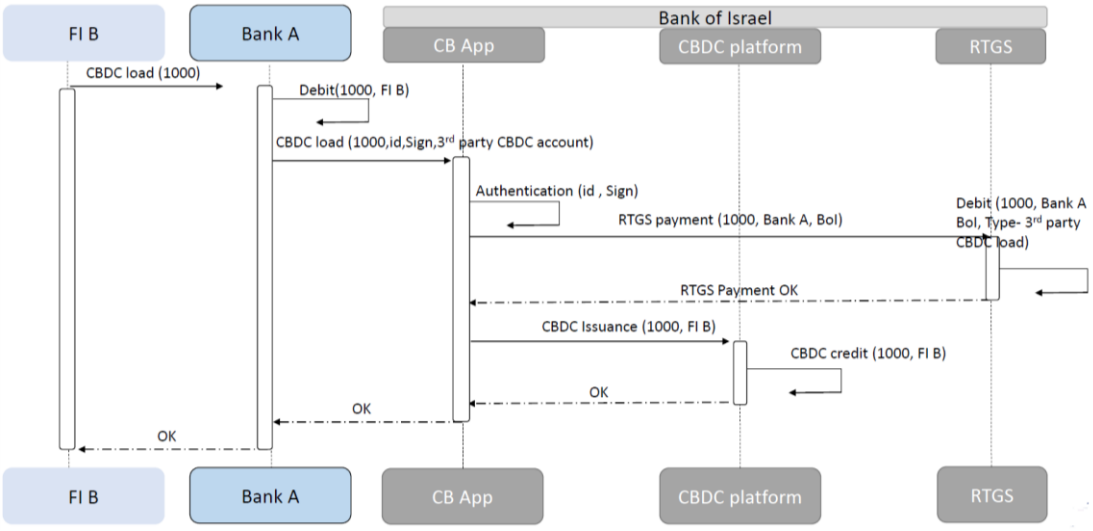


Figure 20 below presents the sequence of the business process in which an FI operating in Configuration B (as described in the table in Section 3) can purchase digital shekels to support the funding operation of its customers.

Figure 20: Purchase of digital shekels by an FI not connected to the RTGS system ("FI B")



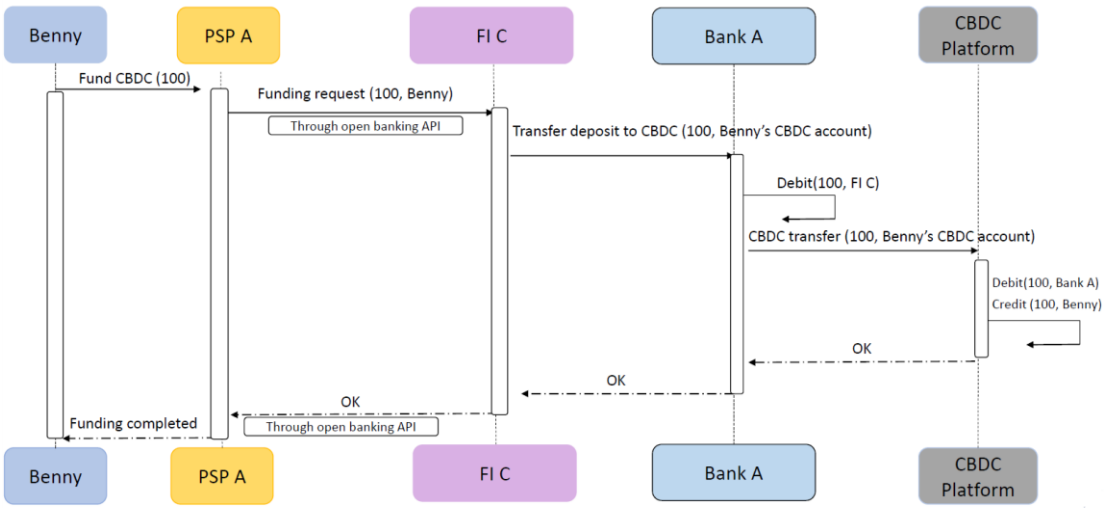
Assumptions:

- FI B is not connected to the RTGS system and uses the connectivity of Bank A where it has an account.
- FI B has a digital shekel account and uses it to support the funding and defunding operations of its customers.

After FI B purchases the digital shekels, it can support the funding and defunding operations of its customers, exactly like Bank A in Figure 19.2.

Figure 21 below illustrates the business process in which an FI operating in Configuration C (as described in the table in Section 3 above) can support the funding operation of its customers even without holding a "stock" of digital shekels.

Figure 21: Funding digital shekels by a customer of an FI that does not hold digital shekels ("FI C")



Assumptions:

- FI C is connected to the RTGS system and uses the connectivity of Bank A where it has an account.
- FI C does not have a digital shekel wallet.
- Benny the end user chose to connect to the digital shekel wallet provided by PSP A to his account with FI C.

The sequence diagrams presented in this document are for purposes of illustration only and do not reflect the final design of the business and technological process.