Bank of Israel
March 2025

Preliminary Design for the Digital Shekel System

Bank of Israel - Bank of Israel's Steering Committee for the Potential Issuance of a Digital Shekel

March 2025

Steering Committee Members: **Andrew Abir (Chair), Limor Goldstein, Lior Georgi, Oded Salomy, Sigal Ribon**

Digital Shekel Project Team: **Yoav Soffer (Project Manager), Tsahi Ben Yosef, Asaf David Margalit, Nir Jacoby, Amir Moshe**

Research Assistants: **Elliot Oster, Anava Sofer**

Contributors to the document sections also include: Yoni Meron (Privacy), Gil Polak (Information Security)
The design process was supported by consultants at Consult Hyperion

Table of Contents

Executive Summary

Similar to many central banks worldwide, the Bank of Israel has been exploring the possibility of issuing a Central Bank Digital Currency (CBDC) since 2017, which in Israel will be called the digital shekel (abbreviated as DS). At the end of 2020, the "Digital Shekel Project" was launched. **Since no decision has been made by the Bank of Israel to ultimately issue the digital shekel**, the project was defined as an "action plan." This means that if future conditions arise where the Bank of Israel assesses that the benefits of issuing a digital shekel outweigh the costs and potential risks, the Bank of Israel will be prepared to implement this plan. At the beginning of 2023, a target was set for the project to present a high-level design document by the end of 2024. This document is now being published to the public to present the design to all stakeholders and receive their feedback. **The document begins with a section titled "How You Can Influence the Design of the digital shekel," describing how stakeholders are invited to provide feedback on various aspects of the design.**

This document presents only a preliminary design - it does not encompass everything necessary to enable the issuance of the DS. Significant processes involving collaboration with many entities in the public and private sectors, as well as a substantial public information campaign, will be required to if it is decided to implement the design. It is important to note that the document presents an "optimal" digital shekel, and it may be necessary to prioritise some of the functionalities and components described in the document based on time, cost, risk management, and benefits considerations. The summary (Chapter 8) briefly outlines the project's work plan, which will culminate in a document recommending to the Governor of the Bank of Israel whether on whether to decide on issuing a digital shekel. Since issuance according to the design presented in the document will likely require legislative changes, such a decision, if made, will also need to be made in collaboration with and supported by the government and the Knesset.

According to the design, the DS is expected to offer a wide range of benefits to users. It will be available to the entire public, including children, foreigners (including tourists), all types of businesses, public institutions, and financial entities. Similar to cash, it will be a universal

means of payment – anyone will be able to pay anyone, and anyone will be able to receive payment from anyone, but with the convenience and advancement of a digital means of payment. Basic uses of the DS for private users will be free, and for businesses, the costs of using it are expected to be significantly lower than with existing digital payments. Payment with the DS is immediate and final, and the DS will also support offline payments, allowing smooth payment transactions even in situations without network connectivity. The level of privacy in the DS will be higher compared to existing digital payments, and similar to cash, it will also offer the possibility of anonymous payments in limited amounts. It will support advanced payment use cases that the private sector will be able to offer to all users – not just financial entities or those operating in decentralised virtual asset – based on the secure infrastructure of the Bank of Israel, in a competitive and open environment that will prevent the creation of "walled gardens." The recently concluded "Digital Shekel Challenge" provided a glimpse into some of the advanced applications that can be offered with the DS, such as "Delivery versus Payment" and "Payment versus Payment," micro-payments, split payments, batch payments, sub-wallets, and wallet status management, among others. Additionally, the DS will be interoperable with other systems, allowing easy conversion between the DS and other means of payment, linking DS payments with trnasactions in other digital asset networks, and enabling users to receive or make payments in the digital shekel even if the other party to the payment does not use the DS.

As the economy becomes digital, the decline in the usability of cash reaffirms the case for maintaining public access to central bank money, in order to ensure the "singleness of money," financial stability, and public trust in "private money," as well as continued competition in the payments system. Issuing a digital shekel primarily addresses this case. Beyond that, it will address several motivations identified by the Bank of Israel in the past, which the design presented in the document supports:

- **Competition.** The DS will allow a wide range of system participants to offer services in the digital shekel and provide an alternative to existing and new means of payment, increasing competition and removing the risk of a "winner-takes-all" phenomenon in the payments system. The possibility of paying interest from the Bank of Israel to DS holders could also increase competition in the deposits market.

- **Innovation.** The DS system will be built from scratch as an innovative system that allows immediate and final payments, supports advanced payment applications, and interoperates with other payment systems and digital asset networks. The collaboration between the public sector, which will lay the infrastructure, and the private sector, which will offer innovative use cases, will ensure innovation while maintaining security and stability.
- **Redundancy.** The DS system will operate as a separate payment system that will not depend on other payment systems for its operation, ensuring the ability to make payments in emergencies or failures in other systems. Support for offline payments will ensure the ability to make payments even in case of system failure or failures to critical infrastructures such as electricity and communication.
- **Cross-border payments.** CBDCs have the potential to streamline and increase competition in cross-border payments, as demonstrated in the Project Icebreaker, in which the Bank of Israel took part. Additionally, cross-border payments can be made in the digital shekel in combination with existing payment systems.
- **Digital payments maintaining privacy.** The level of privacy in the DS will be higher than that of existing digital payments, even if lower than that of cash. The Bank of Israel or any other central entity will not have access to personal identifiable information of wallet holders or the ability to identify their payments. A DS payment can also be of anonymous nature, under conditions to be determined.
- **Combating the "black economy."** The DS will be subject to anti-money laundering and counter-terrorism financing rules. It will be accessible to every resident (individual or corporation) in Israel, including through a basic and accessible access technology, which can also serve those who are reluctant to use existing digital means of payment, helping them to comply with rules on reduction of use of cash and incentivising them to adopt digital payments.

Alongside the benefits, it is important to remember that the DS entails significant risks, such as financial disintermediation, cyber risks, privacy risks, and risks to the central bank's reputation. These risks were considered in the design process, and many design decisions were made to hedge and address these risks.

Below are the main points of the design, described in detail in the document's chapters:

What is the Digital Shekel

The digital shekel is a CBDC that is a liability of the Bank of Israel towards those who hold it, including individuals, businesses, various organisations, and the government. The DS will join physical cash and digital money in bank's reserves at the Bank of Israel, which together form "public money", will be legal tender in Israel with a 1:1 conversion ratio to any other form of Shekel, and will operate alongside the existing range of means of payment. The DS will be usable by the general public (retail CBDC) and financial entities (wholesale CBDC), making it a "multipurpose CBDC".

The Digital Shekel Ecosystem

The ecosystem includes various entities that will fulfil diverse roles. The Bank of Israel, beyond being the sole issuer of the DS, will serve as the system manager and would be setting system rules. The bank (or an entity on its behalf) will also serve as the system operator responsible for the proper functioning of the backend layer. In another role, the Bank of Israel will also act as the supervisor of the digital shekel system, as defined by the Bank of Israel Law: "to regulate the payment and clearing systems in the economy." Alongside the backend layer, several other central services will operate, such as an alias management system and a fraud monitoring system that will help identify and prevent fraud through real-time data analysis. These systems will be designed to maintaining the DS's privacy principles and operate accordingly.

The DS will operate in a two-tier model. Private sector system participants include digital shekel Payment Service Providers (DS-PSPs or PSPs), Funding institutions (FIs), and Additional Service Providers (ASPs). PSPs are responsible for connecting end-users to the digital shekel system and enabling them to make transactions. Without engaging a PSP, an end-user cannot operate in the digital shekel system. Since they do not hold the customer's funds, they do not create the financial risk associated with this, allowing a wide range of entities to operate in the field. FIs will need to enable funding and defunding DS wallets against the account managed with them or against cash. ASPs will offer services such as budget management and advanced payment applications.

The Basic User Journey in the Digital Shekel

The basic user journey in the digital shekel begins with onboarding to the system and creating a wallet. The user can link multiple wallets to their unique identifier and manage them through one or more PSPs. The system will support various access technologies, including smartphones, smart cards, or "stupid" phones, point-of-sale (POS) terminals, and cloud-based interfaces. PSPs will develop and offer access technologies to end-users while adhering to standards and rules set by the system manager.

The end-user can fund the digital wallet in two main ways: against an account with an FI or against cash at ATMs or FI service counters. An online payment transaction in the digital shekel can be performed between any two end-users in the system, subject to necessary checks by the PSP, such as sufficient balance, compliance with anti-money laundering and counter-terrorism financing rules, and fraud monitoring. The system will support micro-payments as well as very high-value payments. Every payment in the digital shekel will be immediate and final, and the system will be available 24/7/365.

The Advanced User Journey in the Digital Shekel

Beyond the basic user journey, the digital shekel includes interoperability with other payment systems in Israel and abroad and with regulated digital asset systems. Interoperability will allow easy and efficient payments between different systems. Thanks to features built into the system's core, such as the ability to lock and release funds under various conditions and based on various mechanisms, system participants will be able to offer advanced and complex payment use cases. The digital shekel will also enable offline payments, independent of communication with the PSP or the backend layer. This capability will be particularly important in areas without communication and in emergencies.

Architecture and Technical Issues

The design presented in the document is "technology-agnostic." Specifically, it does not determine whether the DS will be based on distributed, centralised, or other technology. The logical architecture states that at the core of the digital shekel system are the main database and the settlement engine. The settlement engine updates balances in the main database and performs payment transactions between wallets. The main database includes the minimal information required to settle payments and enforce policy, without storing

personal identifiable information about end-users or information about individual transactions. Alongside the main database, additional databases will exist for operational and statistical analysis, while maintaining privacy principles.

Every transaction in the digital shekel system requires communication between the various entities in the ecosystem. The payment message will include the minimal information required to perform the payment transaction, but the message structure will be designed flexibly so that additional information can be added as needed.

The digital shekel system will be available 24/7/365, with availability as close as possible to 100%. The time to completion and finality of a payment will be no more than a few seconds. Performance requirements will be identical for all participants, so the end-user will enjoy optimal performance regardless of the participant serving them. The system will be designed to be scalable according to the growth in usage.

Policy, Rules, and Regulation

The digital shekel system will be designed with a **privacy-by-design** approach. The Bank of Israel or any other central entity will not have access to personal identifiable information about end-users' activities in the digital shekel. The level of privacy in the digital shekel will be higher than that of existing digital means of payments but lower than that of cash. Participants will not be able to use the information accumulated about users and their activities in the digital shekel system for commercial purposes unless users give clear and informed consent. Anonymous payments, both online and offline, will be possible below thresholds that will be set and in accordance with relevant risk management rules.

The cost of using the digital shekel for basic activities should be low to negligible. Individuals will not pay fees for these activities. PSPs will be able to charge a fee for receiving payments from merchants and will pay an interchange fee to the PSP of the payer. The Bank of Israel will bear its own costs of managing and operating the system.

Users of the digital shekel will enjoy **consumer protection** similar to that provided with other digital means payment. PSPs will be responsible for preventing fraud and compensating customers in case of fraud, according to the rules in the Payment Services

Law. However, offline and anonymous payments will not be eligible for consumer protection.

The digital shekel system must comply with **anti-money laundering (AML) and counter-terrorism financing (CTF)** rules, using advanced technologies and methods to ensure its reliability and prevent economic crime. PSPs will bear the primary responsibility for risk management, including "know your customer" (KYC) processes, monitoring payments, and reporting suspicious activities. The system will be designed to meet international AML standards, with mechanisms for information sharing between PSPs to comply with regulatory requirements.

The digital shekel system will be designed and built according to high **information security** standards to ensure data integrity, user privacy, and protection against threats. The system manager will define policies and procedures for managing system security, while participants will be required to meet stringent standards and conduct independent audits. The system will be designated as critical national infrastructure and will comply with the standards of the National Cyber Directorate.

To hedge against risks to the liquidity of the banking system, as well as negative impacts on the supply and cost of credit, there may be **holding limits** on end users' balances in digital shekels, and in times of crisis concerns, also funding limits. These limits will be determined while considering the impact on user experience and the need for flexibility to adapt to public adoption and long-term trends. Initial simulations of a model designed to calculate the required holding limits for different types of users suggest the magnitude of the necessary limits. The model's results, based on 2024 data, indicate that the required holding limits will allow end users—individuals to small to large businesses, to operate in a wide range of use cases, without the holding limits being a binding constraint. This includes use cases of not every-day payments (such as most payroll payments in the economy and common business-to-business transactions). These findings need to be taken with the necessary caution.

The digital shekel system will allow the functionality for **paying interest** on the held balance, which could enhance monetary transmission, and competition in the deposits market. The decision on paying interest and the rate of interest to be paid will be at the discretion of the

Bank of Israel, according to monetary and macroeconomic conditions, considering the associated risks and complexities.

The document is a preliminary design, and even if a decision were to be made now, it does not describe everything necessary to enable the issuance of a digital shekel at this stage. Upon completion of the preliminary design, the digital shekel project will move to the next phase, and in the years 2025-2026, the project will focus on the following topics:

- In-depth economic analysis of the cost and benefit, opportunities, and risks of issuing a digital shekel.
- Learning and deepening familiarity with the technologies available for implementing the design.
- Adapting the design based on feedback received on this document, public preferences as revealed by studies conducted by the project, and the results of the technological and economic analysis.
- Preparing for the legislative process. The possibility of parallel legislation to ensure the status and respectability of cash will be considered.
- Planning the regulatory framework within which the digital shekel will operate.
- Thorough examination of the implications of wholesale CBDC, and the feasibility that the digital shekel to function as a multi-purpose CBDC.
- Preparing a roadmap for the possible issuance of a digital shekel.
- Preparing a document recommending to the Governor of the Bank of Israel whether to decide to issue a digital shekel. This document will be written towards the end of 2026.

How You Can Influence the Design of the Digital Shekel

This design document is being published to the public to present the evolving design of the digital shekel system to all stakeholders and to receive their feedback in the following ways:

1. **Feedback Questionnaire.** Starting from Chapter 3 of the document, at the end of each section, there is one or more question regarding that section. Through these questions, the project team seeks to gather readers' opinions on the design decisions presented in the document.

Responses to the questions will be submitted via a dedicated online form, accessible at https://forms.gle/4oe8nzKVjhqPLZTT6

(At the beginning of the questionnaire, you can choose to answer in Hebrew or English).

Here are some key points for readers to note:

a. The questions are professionally formulated and pertain to topics relevant to the payments industry, the financial sector, and entities that use payment services (such as retail companies, businesses, consumer organisations, etc.). **However, all readers, without exception**, including academics, civil society, and the general public, **are welcome and encouraged to respond to the questionnaire**.

b. **The questionnaire is not technological.** Most of the questions deal with business issues, the business logic described in the document, and regulatory aspects. Technological feedback can be provided through information received from companies and technology experts, as described in Section 2 below.

c. **The questionnaire is not anonymous.** At the beginning of the questionnaire, respondents must indicate whether they are an individual responding on their own behalf or an organisation, and provide their name and email address. This information will be used by the project team to analyse the responses correctly and may also allow for follow-up to seek clarifications or additional information if necessary. The Bank of Israel will not disclose the identities of the respondents, nor will it publish positions or responses that can be attributed to specific respondents.

d. The Bank of Israel may publish aggregate analyses of the questionnaire responses but does not commit to doing so.

e. **You can choose which questions to answer and are not required to complete the entire questionnaire.** You can choose to answer sequentially according to the document or select specific topics in the questionnaire (according to the selection menu) and address only those. From any section in the questionnaire, you can "jump" to any other section or to the questionnaire's end page.

f. The questions from the questionnaire are integrated into the document to facilitate addressing them in the context in which they were written, although the responses will be submitted via a dedicated form. It is important to note that, in addition to the questions asked, **the form itself allows for additional comments on each section.** After the list of questions for each section, there is an option for additional comments under the heading "Additional comments for this section."

g. **Responses to each question are limited to 1,500 characters** (approximately 250 words).

h. The questionnaire will be open for responses **until April 30, 2025.**

i. **Clarifications and Disclaimers** - It should be noted that the Bank of Israel reserves the right to utilise any information submitted in response to the questionnaire, subject to the provisions of Section C above, and is under no obligation to accept any of the submitted positions, if any. Furthermore, this request should not be interpreted as a commitment by the Bank of Israel to any party.

2. **Receiving Information from Companies and Technology Experts.** In a few weeks, the Bank of Israel will publish a series of Requests for Information (RFI) regarding the technological implementation possibilities of key services and capabilities in the digital shekel system, as detailed in the design. Technology companies and technology experts will be able to provide feedback on the recommended technological implementation of one or more components for which information is requested. The initial response will be in writing, and subsequently, the Bank of Israel will consider whether and how to continue the dialogue with some or all respondents, at its discretion.

Detailed information about the components for which RFIs will be published, the response process, and the conditions under which it will be conducted will be published later.

It should be emphasised that those intending to respond to the technological RFIs are not precluded from also responding to the questionnaire described in Section 1.

Glossary

"The Beginning of Wisdom is the Definition of Terms" ~ Socrates

Entities in the Digital Shekel System

1. **End Users -** Anyone who can hold a balance and perform payment transactions with the digital shekel: individuals and organisations (businesses, non-profits, government offices, etc.). Participants in the system may also hold a wallet(s) and act as end users. An end user is the owner of the digital shekels in their wallet.
2. **Indirect End User -** An entity that has been granted permission by the end user who owns the wallet to use their digital shekels. The indirect user will operate in a separate wallet linked to the identifier of the direct user, to which transactions made by and under the control of the indirect user will be attributed. The indirect user will join only with the approval of the direct user, and their details will be kept by the PSP providing service to the indirect wallet (examples: children under the age at which they can hold a wallet directly, branches or organs of a business, etc.).
3. **Participant -** An organisation that plays a role in the digital shekel system and is bound by the system's scheme rules. So far, the following types of participants have been defined for the digital shekel system:
    - Digital Shekel Payment Service Provider (DS-PSP)
    - Funding Institution (FI)
    - Additional Services Provider (ASP)
4. **System Manager -** The entity that defines the scheme rules and is responsible for the proper management of the system, including supervising the various participants in their activities concerning the scheme rules, resolving disputes between participants, etc. The Bank of Israel is expected to fulfil this role.
5. **System Operator -** The entity that operates the technological infrastructure according to the scheme rules and the terms of engagement with the system manager. The system operator will be the central technological entity with which most technological engagements of the various entities will be conducted. The Bank of Israel, or an entity appointed by it, is expected to fulfil this role.

6. **Funding Institution (FI) –** Financial entities licensed by a financial regulator that manage payment accounts for the public outside the digital shekel system and will allow their customers to convert money from their account balance to DS (funding) and vice versa (defunding). Examples include commercial banks, the Postal Bank, credit unions, financial asset service providers, etc. Some of these entities will also support the conversion of cash to DS and vice versa for all end users of the digital shekel. Different models for FI activity may exist, depending on whether the FI has access to the RTGS and whether it relies on its own digital shekel balance or that of another FI to perform the funding and defunding processes for its end users.
7. **Digital Shekel Payment service provider (DS-PSP) –** The entity responsible for providing the necessary technological and business framework to connect end users to the digital shekel system (conducting KYC procedures, providing and recovering access technology to the system, customer service, etc.) and enabling end users to perform transactions. Without engagement with a payment service provider, an end user cannot operate in the digital shekel system.
8. **Additional Services Provider (ASP) –** An entity of this type can provide optional additional services to end users, such as budget management, analytics services for businesses, payment insurance, advanced payment applications (e.g., conditional payments), etc.
9. **Default Payment Service Provider –** A payment service provider that must provide basic payment services in DS to anyone eligible for a digital shekel wallet. There is no necessity for such an entity to exist.

Business Terms

1. **Retail Central Bank Digital Currency (rCBDC) –** A digital currency issued by the central bank, representing a direct liability of the central bank, intended for use by the general public.
2. **Two-Tier Model –** An operational model for the rCBDC system where end users' access to the system is based on engagement with payment service providers who supply the necessary technological, service, and business framework for this access.

3. **Smart Money –** Digital money that, beyond being a simple database entry like "classic" money, is managed in a system that allows for advanced use cases, such as smart contracts, DeFi, conditional payments, and more.
4. **Wholesale Central Bank Digital Currency (wCBDC) –** An upgrade of the RTGS system to smart money that can operate 24/7/365. It has built-in programmability and connectivity to other systems (DLT and others). According to the BIS, wCBDCs are intended for use in transactions between central banks, commercial banks, and other financial institutions, meaning they will play a role similar to that of reserves or clearing accounts currently held at central banks. However, they can enable financial institutions to access new functions powered by tokenisation, such as composability and programmability.[1]
5. **Payment Transaction –** The transfer of digital shekels from one wallet to another wallet(s).
6. **Funding/Defunding –** The conversion of other forms of New Israeli Shekels (e.g., deposits in an FI, as well as cash) into DS. The result of a funding process is that the balance in the end user's digital shekel wallet increases, and their balance with the FI (or their cash balance) decreases. Defunding is the reverse of funding.
7. **Issuance/Redemption –** The creation/deletion of new/existing digital shekels by the Bank of Israel, resulting in a change in the amount of DS in circulation.
8. **Waterfall Mechanism –** A process in which digital shekels are automatically defunded from the digital shekel wallet if the balance exceeds the maximum holding amount defined by the holding limit (if defined) or according to the end user's preferences. This allows the user to receive payments into the digital shekel wallet even if the payment increases the balance beyond the holding limit. A wallet not linked to an FI cannot use this mechanism.
9. **Reverse Waterfall Mechanism –** A process in which the digital shekel wallet is automatically funded if there is an insufficient balance to perform a transaction, or if the balance falls below a certain threshold defined by the user. This mechanism can allow for payment actions in amounts higher than the holding limit.

[1] Composability is the ability to bundle multiple actions so that they are executed following a single transaction command.
Di Iorio, A., Kosse, A., & Mattei, I. (2024). Embracing diversity, advancing together-results of the 2023 BIS survey on central bank digital currencies and crypto.

10. **Conditional Payment –** A payment that is executed (automatically or initiated) only if one or more predefined conditions are met. These can be conditions known to the system, such as time and usage characteristics, or external conditions, such as a delivery versus the payment. Various technological and business mechanisms exist for managing a conditional transaction process. In some mechanisms, a certain balance may need to be locked when the transaction is closed, and released to the payee when the condition or trigger is met.
11. **Offline Payment –** A payment in a situation where both parties, the payer and the payee, are not connected to the backend of the DS system, and the payment is transferred via an electronic message between their access technologies.
12. **Synchronous Payment –** A payment involving both user interfaces (the payer and the payee) at the time of the transaction. For example, the payee's user interface sends a payment request, and the payer approves the request through their interface.
13. **Asynchronous Payment –** A payment involving only the payer's user interface at the time of the transaction. No action is required from the payee for the payment to be executed. However, the payee can receive a notification of the transaction's completion.

Technological Terms

1. **Access Technology –** The hardware and/or software that allows end users to perform payments and manage their digital shekel balances. An access technology includes a secure container and usually also a user interface.
2. **Unique Identifier –** A one-to-one identifier issued for each end user registered in the digital shekel system, to which the wallets of that end user are linked. The unique identifier lacks identifying features of the end user and cannot be used to identify the user.
3. **Alias –** An easy-to-remember or retrieve nickname, such as a name, phone number, or email address of the end user linked to their wallet. The alias allows payments between end users without needing to specify the identifier, which may be a complex sequence of letters and numbers.

4. **Digital Shekel Wallet –** A compartment in the digital shekel database where balances of digital shekels (and only digital shekels) are recorded. The wallet is used to perform funding, defunding, and payment transactions in the digital shekel system. There cannot be a negative balance in the wallet. The wallet is linked to the user's unique identifier, and the user's access to the wallet will be through a payment service provider. A user can hold multiple digital shekel wallets linked to their unique identifier. They can link a wallet or multiple wallets to multiple payment service providers or link multiple wallets to a single payment service provider.
5. **Offline Digital Shekel Wallet –** A hardware component where balances of digital shekels are recorded, used to perform funding, defunding, and payment transactions in the digital shekel system offline. There cannot be a negative balance in the wallet. Unlike an online digital shekel wallet, each offline wallet can only be linked to one PSP.
6. **Backend Layer –** The system components required by the system operator to perform its functions in the digital shekel system, including the necessary and/or derived databases from these actions (including the main database containing the balances in all end-user wallets). In particular, the backend will include the "settlement engine" - the component that enables the transfer of digital shekels as a result of a payment between two wallets - and the main database.
7. **Offline Digital Shekel Issuance Engine –** A component in the backend layer that communicates through the PSP to the user's offline digital shekel wallet and issues offline DS into it, while simultaneously "redeeming" DS from the user's online wallet.
8. **Account-based System –** An architecture for recording liabilities to end users as balances in accounts, and payment actions as debit in the payer's account and credit in the payee's account for the same amount.
9. **Token-based System –** An architecture for recording liabilities to end users by computer files (tokens) of various values, with mapping linking the tokens to their owners.

Abbreviations and Acronyms

DS - Digital Shekel

AML - Anti-Money Laundering

ATM - Automated Teller Machine

CBDC - Central Bank Digital Currency

CDD - Customer Due-Diligence

CFT - Combating the Financing of Terrorism

DvP - Delivery Vs Payment

ECB - European Central Bank

EMV - Europay, Mastercard, Visa (International standard for smart payment cards and terminals supporting them)

IoT - Internet of Things

KPIs - Key Performance Indicators

KRIs - Key Risk Indicators

KYC - Know Your Customer

NFC - Near-Field Communication

PET - Privacy-Enhancing Technologies

PII - Personally Identifiable Information

PvP - Payment Vs Payment

RPO - Recovery Point Objective

RTO - Recovery Time Objective

- **User Abbreviations** – Private (P), Business (B), Government/Public (G), Financial Institution (F).

1. Introduction

Similar to many central banks worldwide, the Bank of Israel has been exploring the possibility of issuing a Central Bank Digital Currency (CBDC) for several years, which in Israel will be called the digital shekel (abbreviated as DS). In 2018, a report was published by the interdepartmental team for the study and examination of central bank-issued digital currencies.[2] At the end of 2020, the Governor of the Bank of Israel appointed the Steering Committee for the possible issuance of the digital shekel, chaired by the Deputy Governor, and the "Digital Shekel Project" was launched. **Since no decision has been made by the Bank of Israel to ultimately issue the digital shekel**, the project was defined as an "action plan." This means that if future conditions arise where the Bank of Israel assesses that the benefits of issuing a digital shekel outweigh the costs and potential risks, the Bank of Israel will be prepared to implement this plan.

Initially, the project mainly focused on self-study – covering technological issues, business topics, and the possible implications of issuing a digital shekel on the financial system, the payment system, and the economy as a whole. Over the past four years, a significant amount of information has been shared with the public about the project's progress on the Bank of Israel's website.[3] In late 2022, the project began to focus on the initial design of the digital shekel, which emerged from the draft model presented in a document published by the Steering Committee to the public in 2021.[4] Simultaneously, the bank continued to conduct technological experiments, some independently and some in collaboration with the BIS and other central banks. At the beginning of 2023, the Steering Committee set a target for the project to present a high-level design document by the end of 2024. This document was discussed by the Steering Committee during December 2024 and is now being published to the public.

The digital shekel, if and when issued, will be a digital means of payment available to the entire public: residents of Israel – including children, adults, businesses, public entities,

[2] Bank of Israel (2018). Report of the team to examine the issue of Central Bank Digital Currencies
[3] Bank of Israel – The Digital Shekel.
[4] Bank of Israel (2021). Digital Shekel of the Bank of Israel: Potential Benefits, Draft Model, and Issues to Examine.

financial institutions, any other legal entity – and even non-residents of Israel. Unlike the wide variety of types of digital money and digital means of payment that already exist today, such as bank accounts, payment apps, and debit cards, the digital shekel will be a liability of the Bank of Israel to the holder, similar to cash, rather than a liability of a private-commercial entity. The first question we must ask when considering the issuance of a digital shekel is – why? What is the added value of the digital shekel over the existing range of means of payment?

Humanity is undergoing a digital revolution. Many products and services that were previously consumed only in a physical or analogue form are now provided digitally. Various sectors of the economy are disappearing or making adjustments to remain relevant. Central banks have provided the most common and usable means of payment for hundreds of years – physical cash, in the form of banknotes and coins, and the Bank of Israel has done so since it was established 70 years ago. Even in the digital age, cash remains highly important for large segments of the population (e.g., those with low digital literacy or disabilities that make it difficult to use digital means of payments); and in various scenarios, such as extreme emergencies or natural disasters. The Bank of Israel does not intend to stop issuing cash. However, as the economy becomes digital and digital means of payment become more prevalent, convenient, and secure, the usability of cash is declining, and means of payment based on money that is not a central bank liability ("private money") are taking its place. Many central banks, including the Bank of Israel, are asking themselves: will they disappear from the landscape in terms of offering a means of payment for public use, as many product and service providers are disappearing? Or should they make adjustments to remain relevant, like some industries are doing?

A decline in the usability of cash, to the point of its near disappearance, means leaving the field of publicly available means of payment solely to the private sector. This could have three main implications:

- **Jeopardize the principle of "singleness of money."** Economic history shows that in situations where only private institutions issued money for public use, there were events where money issued by one institution was not at par with that of another

(e.g., in the United States in the 19th century).[5] This undermines the ability of money to serve one of its central roles – to be a unit of account. The existence of central bank money as a monetary anchor, to which all other types of money are easily, quickly, and cheaply convertible, ensures that all types of money are equal in value.

- **Risks to financial stability.** Central bank money is the safest asset in the economy. Unlike private money, holding it is not associated with credit risk. One reason the public is indifferent to this risk when holding private money is the fact that whenever they withdraw cash, they see that the singleness of money is maintained, and their money in the bank is always convertible to the risk-free money of the central bank. If the public is unable to, at will, withdraw and use central bank money, this could undermine public confidence in private money.[6]
- **Harm to competition.** Cash exerts competitive pressure on private means of payment. Its declining relevance could lead to a less competitive payment market, especially where the market is relatively concentrated.

It is important to emphasise that there is no consensus regarding the magnitude of the implications mentioned above, and their validity may vary over time and between jurisdictions. Uniformity of money can be maintained even if types of private money are convertible to each other through the reserves at the central bank and the RTGS system. It can be argued that central bank digital money ensures the principle of uniformity, even if it is only wholesale – that is, available only to financial institutions and not to the general public. Public confidence in the banking system is largely ensured by the effective supervision exercised by the Banking Supervision Department at the Bank of Israel. The impact on competition can also be mitigated through appropriate regulation. However, this is not a laboratory experiment, and it may indeed be difficult to assess the implications of the declining relevance of central bank money in real-time.

Beyond the need to maintain public access to central bank money in the digital age, the Steering Committee identified six possible motivations for issuing a digital shekel in a document published in 2021, considering the relevant conditions of the State of Israel.

[5] Elwell, C. K. (2011). Brief history of the gold standard (GS) in the United States.

[6] For further reading: Panetta, F. (2021). Central bank digital currencies: a monetary anchor for digital innovation. *Speech at the Elcano Royal Institute, Madrid.*

Below, we will review these motivations and briefly discuss how the design presented in this document supports them:

1. **Creating an efficient and secure alternative to existing and new means of payment in the digital age.** The digital shekel has the potential to increase competition in the payment system and eliminate the fear of a "winner-takes-all" phenomenon in any part of the payment system, whether by an existing entity or by entities offering private money using new technologies. Since the DS is a liability of the Bank of Israel, a wide range of private sector system participants will be able to offer payment services using it,[7] without bearing the financial risk of holding the money. Therefore, they will be exempt from stringent regulation in this area. Payment Service Providers can offer innovation in payments without compromising (and even enhancing) public confidence in money. Paying interest from the Bank of Israel to DS holders may also increase competition in the deposit market, as described in section 7.7 of the document.
2. **Creating an innovative infrastructure that ensures the payment system's adaptation to the needs of the future digital economy.** The DS payment system is an innovative system built from scratch. Payments are immediate and final. Chapter 6 of the document describes the extensive capabilities that will enable the system to support advanced payment applications, with interoperability with other payment systems as well as with other digital asset networks that are currently developing and will develop in the future. The Digital Shekel Challenge,[8] which recently concluded, demonstrated several innovative use cases by private companies that the DS system will be able to support. The collaboration between the public sector, which will lay the infrastructure equally for all participants and ensure its availability and safety, and the private sector participants, who can offer innovative use cases, is a recipe for the system's success in offering innovation and progress while maintaining high standards of security and stability.
3. **Ensuring the redundancy of the payment system and its proper functioning in emergencies or failures.** The DS system will operate as an additional payment

[7] As described in Chapter 3 of this document.
[8] Bank of Israel – The Digital Shekel Challenge.

system that will not depend on other payment systems for its operation.[9] The central settlement engine will be under the responsibility and management of the Bank of Israel. Communication between the participants and between them and the Bank of Israel will not depend on existing payment systems. Support for offline payments will ensure the ability to make payments even in case of a system failure or in case of national infrastructure failures, such as electricity and communication.

4. **Creating an efficient and low-cost infrastructure for cross-border payments.** Central bank digital currencies have the potential to streamline and increase competition in cross-border payments, as demonstrated in Project Icebreaker,[10] in which the Bank of Israel took part. However, so far, there is no international initiative for the connectivity of retail CBDC systems, as demonstrated in that project. Section 5.1.2 of this document describes how the design supports at least the ability to make cross-border payments in the digital shekel in combination with existing payment systems and how the design will ensure that if international arrangements for connecting CBDC systems are established, the digital shekel will be able to integrate with them.
5. **Maintaining the public's ability to make digital payments while preserving a certain level of privacy.** The Two-tier model ensures that while end users' DS wallets will be represented in the main database managed by the Bank of Israel, neither the Bank of Israel nor any other central entity – governmental or private – will have access to personal identifiable information of end users. This information will be held only by the Payment Service Providers. If such information is requested, it will be obtainable from them only according to the law (e.g., by law or court order) – as is currently the practice. The Bank of Israel will not have a database that allows the attachment of identity to DS wallet ownership. Making a payment in DS can be of anonymous nature. Each user will be able, up to amounts to be determined in the future, to make payments, whether online or offline, so that the identity of the payer, the payee, or the context of the payment will not be visible to any other entity.

[9] The system depends on other systems for wallet funding and defunding, but not for payment actions, as long as these start and end within the DS system and do not involve interoperability with other systems.

[10] Bank for International Settlements, Bank of Israel, Norges Bank, Sveriges Riksbank, & BIS Innovation Hub Nordic Centre. (2023). Project Icebreaker: Breaking new paths in cross-border retail CBDC payments.

Section 7.1 describes several additional features that will ensure the privacy level of the DS is higher than that of existing digital means of payment, even if lower than that of cash.

6. **Supporting the government's policy to reduce the use of cash and combat the "black economy."** As a digital means of payment, the DS will be subject to anti-money laundering and counter-terrorism financing rules. As described above, enforcement authorities, including the police and tax authorities, will be able to view information about DS users' activities only according to legal provisions. The Bank of Israel will ensure that the DS is accessible to every resident (individual or corporation) in Israel. One way to do so is by setting a standard for a basic and accessible access technology, which can also serve those who are reluctant to use existing digital means of payments, thereby helping those parts of the population comply with cash usage reduction rules and adopt digital means of payments.

These, then, are the motivations of the Bank of Israel for the possible issuance of a digital shekel. The question arises, what about the general public? Why would households and businesses, that already have a variety of payment options and trust the stability of the banking system despite the credit risk inherent in private money, want to use the digital shekel?

The DS is expected to offer a wide range of benefits to all segments of the population. It will be available to the entire public, including children, foreigners, all types of businesses, public institutions, and financial entities. Similar to cash, it will be a universal means of payment – anyone will be able to pay anyone, and anyone will be able receive payment from anyone, but with the convenience of a digital means of payment. Like cash, payment in the DS is immediate and final, a feature not currently offered in small retail payments.[11] The DS will support offline payments, ensuring that even in situations without network connectivity, payment transactions can be completed smoothly. Its level of privacy will be higher compared to existing digital means of payments, and similar to cash, it will also offer the possibility of anonymous payments, albeit in limited amounts, while adhering to anti-money laundering and counter-terrorism financing regulations. The DS will support advanced

[11] For further details and a distinction between the DS and existing systems that provide immediacy and finality, see Box 4.

payment scenarios – some of which exist today but will be universally available on the secure infrastructure of the Bank of Israel – and some that do not exist today. Thus, the DS will enable every end user – private, business, governmental, or financial – to benefit from advanced applications, some of which are currently available only to financial entities or in with decentralised assets, such as delivery versus payment and payment versus payment, micropayments, split payments, batch payments, sub-wallets, and wallet status management, among others. All these are described in section 5.2, and some were successfully demonstrated in the "Digital Shekel Challenge." The DS will be interoperable with other payment systems, allowing users to receive or pay in digital shekel even if the other party to the payment does not use the digital shekel.

The DS is expected to operate within what is called a "Two-tier model" While financially, the DS represents a liability of the Bank of Israel to the end user holding it, users' access to the system will be facilitated through private sector participants, particularly Digital Shekel Payment service provider. These entities, unlike the central bank, are capable of managing the necessary interfaces with end users, conducting the required checks under anti-money laundering rules, providing the necessary customer services, and developing advanced capabilities and innovative user interfaces in a competitive environment. The ability of these entities to make commercial use the information they collect will be limited and conditional on the explicit consent of the user. However, beyond the basic services in the digital shekel, payment service providers and Additional services provider will be able to offer a wide range of advanced payment services, as well as link payment services – both basic and advanced – to other areas of activity they engage in, such as financial services, retail activities, e-commerce, and more. These activities will enable system participants to build a sustainable business model for their operations in the digital shekel, and through them, the digital shekel can be leveraged to creating new economic activity.

It is important to note that alongside the many benefits, the digital shekel also entails significant risks, especially if not carefully designed. The main risk that of financial disintermediation resulting from the conversion of a significant portion of public deposits in banks to the digital shekel. A poorly designed system could also yield cyber risks, privacy risks, and reputational risks for the central bank. These risks have been considered

throughout the design process, and many of the design decisions reflected in the document aim to hedge and address these risks.

This document presents an initial design of the digital shekel, and it is the product of over two years of work by the project team, under the guidance of the Steering Committee. During the design process, about twenty different and diverse areas were examined and researched:

- Principles for Establishing Acceptance
- Interoperability
- Principles for System Management
- Information Security
- Privacy
- System Data Model
- Cost Structure in Payment Transactions
- Holding Limits
- Definition of User Base
- Cross-Border Payments
- Logical Architecture
- System Performance
- Access Technologies
- Advanced Payments
- Immediacy and Finality
- Offline Payments
- Anti-Money Laundering and Counter-Terrorism Financing
- Consumer Protection

In each topic, following the analysis, the project team brought the design decisions and the resulting requirements to the Steering Committee for approval. Once approved by the Steering Committee, hundreds of decisions and requirements were documented, which are reflected in this document. Chapter 2 briefly defines what the digital shekel is. Chapter 3 deals with the digital shekel ecosystem and the roles of the various entities operating within it. Chapter 4 presents the basic user journey – joining the digital shekel, funding the wallet,

and performing a basic online payment. Chapter 5 presents the advanced user journey – interoperability with other systems, advanced payment applications, and offline payments. Chapter 6 presents the logical architecture and several technical topics. It should be emphasised that the design so far is "technologically-agnostic" and avoids, to the extent possible, directing towards any specific technology. Chapter 7 presents a wide range of policy, rules, and regulatory issues. As mentioned, the document is a preliminary design, and even if a decision were to be made now, the document does not describe everything necessary to enable the issuance of a digital shekel at this stage. Chapter 8 details the planned steps.

It is important to note that this document presents the "optimal" digital shekel, from the perspective of the Steering Committee and the project team. The DS described in the document supports a very wide range of use cases, by a wide range of system participants, and for the benefit of a wide range of end-user types. Typically, payment systems are not built in a day. It may be necessary to prioritise some of the capabilities and components described in the document, due to time, costs, risk management, and other considerations. This prioritisation could be reflected in a decision to issue the digital shekel with only some of the features and add additional features in the future, or alternatively, in a decision to limit the digital shekel so that only some of the described features are implemented.

This document is being published to present the design to all stakeholders and potential partners and to receive their feedback. **The summary chapter describes in detail how various entities can to respond to the design document.**

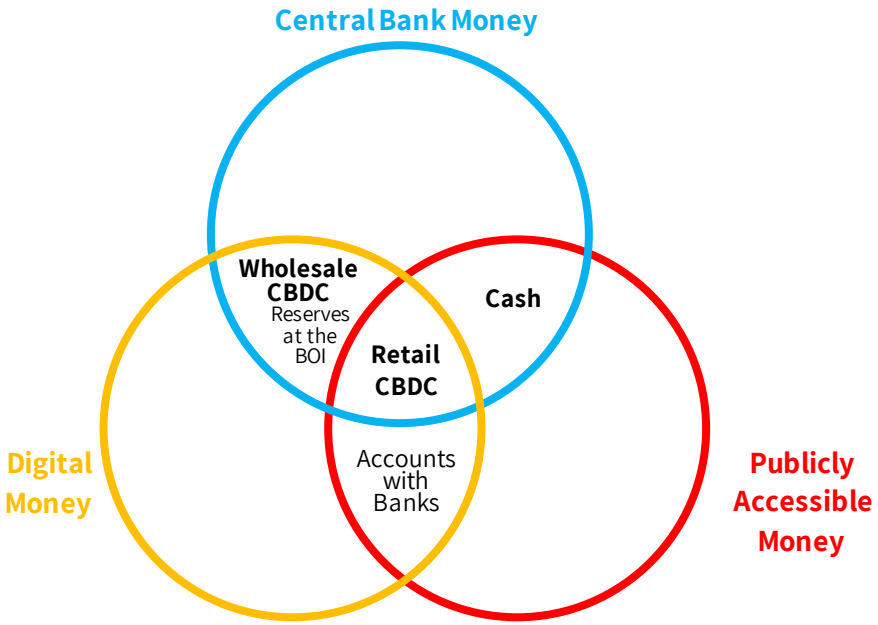
2. What is the Digital Shekel

The Digital Shekel (DS) is a Central Bank Digital Currency (CBDC) that represents a liability of the Bank of Israel to its holders, including individuals, businesses, various organisations, and the government. The DS will join physical cash and reserves at the Bank of Israel that together constitute "public money", and will be legal tender in Israel with a 1:1 conversion rate to any other form of Shekel.

The Digital Shekel (DS) - a Central Bank Digital Currency (CBDC) - is a digital means of payment that represents a liability of the central bank to its holders – individuals, businesses, various organisations, the government and its branches, and more. The DS will join other forms of money that are liabilities of the Bank of Israel – physical cash, and digital money in the commercial bank's reserves[12] at the Bank of Israel – together these constitute the monetary base, or "public money." The DS will be added to the variety of existing means of payment today – cash, and means of payment based on "private money" – bank transfers, debit cards, payment apps, checks, and more. The DS will be legal tender in Israel, thus its status will be equivalent to that of banknotes and coins which constitute legal tender in physical money. Similar to cash and any other payment system using central bank money, payment in the digital shekel will be immediate and legally defined as final payment. The digital shekel will be convertible at a 1:1 ratio to any other form of shekel – whether it is a liability of the Bank of Israel (cash, or reserves) or a liability of a commercial financial entity (e.g., a current account balance in a bank).

[12] The government also maintains accounts at the Bank of Israel, and recently the Bank of Israel has allowed payment companies access to the RTGS system and to hold payment accounts within two days.

Figure 1: The Digital Shekel and Other Types of Money in the Economy



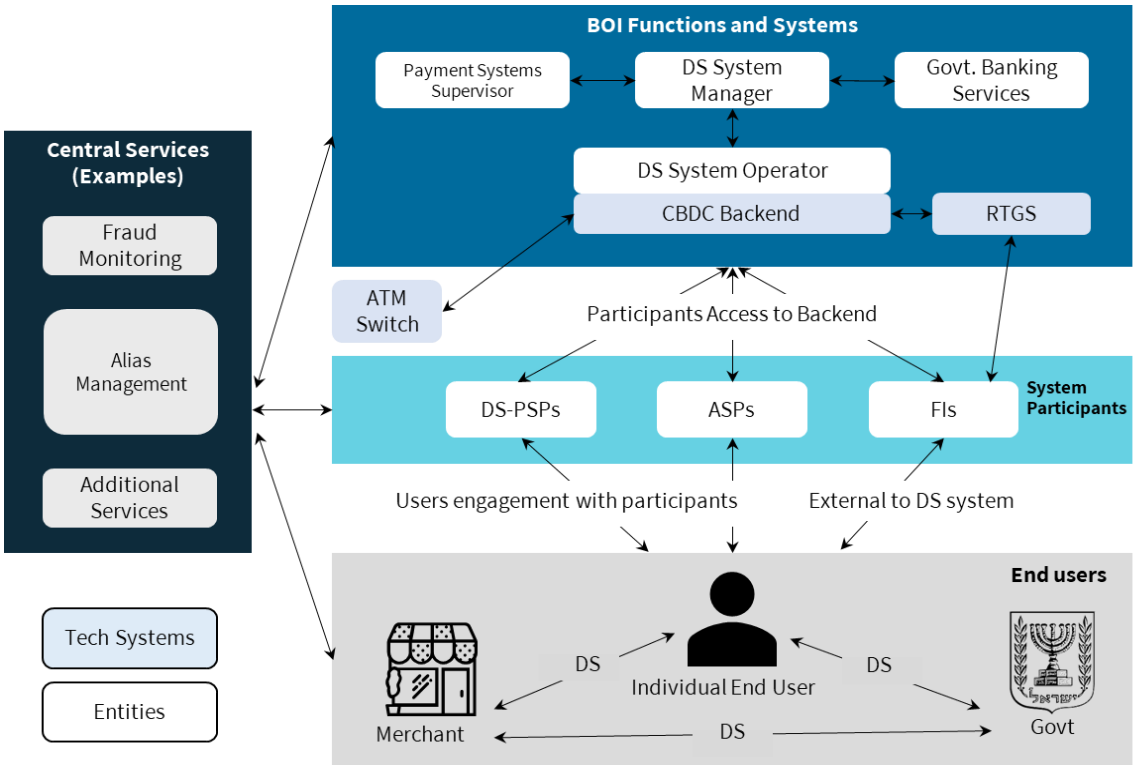
It is common to distinguish between a central bank digital currency intended for use by the general public, with an emphasis on individuals and merchants (Retail CBDC), and one that can only be used by banks and sometimes additional financial entities (Wholesale CBDC). This document proposes that the digital shekel could be used by both the general public and financial entities – further details on this topic can be found in Box 2.

3. The Digital Shekel Ecosystem

Various entities will operate in the digital shekel system fulfilling different roles, all of which together comprise the ecosystem of the digital shekel.

In this chapter, we will detail the types of entities, their roles, and how they will operate within the digital shekel system.

Figure 2: The Digital Shekel Ecosystem



3.1. Bank of Israel

The Bank of Israel will be the issuer of the digital shekel, set the rules for the digital shekel system, serve as the system manager, and oversee it. The system operator could be the Bank of Israel itself or an entity operating it on its behalf.

3.1.1. Issuer of the Digital Shekel

The Bank of Israel is the issuer of the digital shekel. The authority to issue or redeem (or, by analogy to physical cash, "burn") digital shekels will be vested solely in the Bank of Israel or an entity authorised by the Bank. In this role, the Bank of Israel will need to manage the balance of digital shekels in circulation at all times and maintain tools to track it.

3.1.2. Manager of the Digital Shekel System

The Bank of Israel also serves as the manager of the digital shekel system. As such, it will set the system rules ("scheme rules"), establish principles for the system's operation (participant liabilities, SLAs, basic principles for participant interactions with end users, access technology, technical requirements, etc.), and the risk management rules that will bind the participants, as well as the liabilities of the system operator. As the system manager, the Bank will define mechanisms for resolving disputes between system participants and between participants and the system operator, and enforce these rules and mechanisms.

3.1.3. Operator of the Digital Shekel System

The system operator could be the Bank of Israel itself or an entity appointed by the Bank of Israel to operate it (e.g., a technology provider). The system operator is responsible for the operation of the backend layer (see section 6.1). It will ensure the proper functioning of the system as a whole and continuously monitor its performance according to metrics set by the system manager.

3.1.4. Supervisor of the Digital Shekel System

The Bank of Israel will also serve as the supervisor of the digital shekel system, by virtue of its role defined in the Bank of Israel Law: "to regulate the payment and clearing systems in the economy." Supervision of the digital shekel system will be carried out by the Payment Systems Supervision Division at the Bank of Israel.

3.1.5. Banker of the Government Digital Shekel System

Another role of the Bank of Israel, defined in the Bank of Israel Law, is to serve as the banker of government. This role is performed by the Banking Services Unit in the Accounting Department of the Bank of Israel. For the government and its various branches to make and receive payments in the digital shekel, this unit will need to serve as both an FI. (see section 3.3.2) and a PSP (see section 3.3.1) for the government.

Questions – Roles of the Bank of Israel in the Digital Shekel System:

1. This chapter outlines the division of responsibilities between the Bank of Israel and other entities within the digital shekel system. Does the proposed functional division effectively meet the system's needs? Are there additional entities or types of organisations that should be included in the ecosystem?

3.2. Central Services

Alongside the backend layer, several central services will operate to address various needs of the digital shekel system. Some of these services may be managed by the Bank of Israel, while others may be managed by different entities either public or private.

Below are descriptions of two central services that will be required:

3.2.1. Alias Management System

Making payments using an alternative identifier (Alias) is an important feature expected to enhance the convenience of performing payments and prevent errors. In the digital shekel system, it is important that the Alias is issued by a central mechanism and not dependent on the identity of the PSP managing the end users wallet. This mechanism will be able to link the identity of the end user (individual – by ID number, corporation – by registration number, etc.) to a unique identifier. To ensure the privacy principles of the digital shekel, this system

will operate outside the Bank of Israel,[13] in a way that does not allow the bank to link the wallet and its activities to the end user's identity or their Alias. However, the Bank of Israel will define the structure of the Alias, which will be issued according to principles which were developed by the Bank of Israel this matter.[14] This system will also be able to assist the PSP in identifying the user during the process of onboarding to the digital shekel.[15]

Questions – Alias Management System:

2. Do you believe that a system enabling end users to initiate actions within the digital shekel system using a recognised and simple alternative identifier – such as a mobile number or email address – is important? Are there other alternatives that could ensure a positive user experience and smooth transition between payment service providers without compromising the privacy principles of the digital shekel?
3. Is it important for such a system to operate independently of the Bank of Israel? If so, where should it be managed?

3.2.2. Fraud Monitoring System

A central fraud monitoring system will be established and operate alongside the settlement engine, assisting PSPs in identifying and preventing misuse events, in addition to the systems independently operated by the PSPs (see section 0). The nature and role of this system will be determined by the system manager (within the framework of scheme rules or legislation). The system manager will establish this system. The manner in which it will be established and operate will be determined at a later stage, with the guiding principle being that the Bank of Israel will not have access to the information received in this system.

The role of the system will be to assist PSPs in managing and reducing fraud risks by providing real-time indications of the risk level for each payment transaction that it would

[13] For example, it could operate as part of the national identification system managed by the Digital Israel Bureau.
[14] Bank of Israel (2023) – The principles for transferring money immediately between accounts via an identifying detail such as a mobile phone number or email address have been formulated.
[15] See section 4.1.

be requested to evaluate. The system will analyse a wide range of data (but in any case, not personally identifiable information (PII) of DS users), such as activity patterns, transaction history, geographical characteristics, wallet age, the "network" of wallets interacting with the paying wallet, and more. By using advanced artificial intelligence and machine learning technologies, the system will identify anomalies and suspicious behaviour patterns and provide the PSP with a "risk score" for each specific transaction. It should be emphasised that the responsibility for preventing misuse remains with the PSPs, and this system will assist them by providing indications based on information they do not possess.

It is important to emphasise that the indication provided by the central system will be an additional layer in the PSPs' risk management process but should not be the decisive factor in their decisions. They will be able to combine the information received from this system with their internal monitoring systems and professional judgment.

When a PSP receives a payment transaction request from a user, it can route the request to the central system to receive an indication of the transaction's risk level. The indication, combined with its internal information about its customer, will allow the PSP to make an informed decision regarding the payment transaction: approve it, decline it, or require additional verification from the payer. This combination will enable a more comprehensive and efficient approach to fraud prevention while maintaining operational flexibility and service provider responsibility.

The central system will operate dynamically and continuously, learning and improving from all transactions performed in the digital shekel system. This will allow for better identification of new fraud patterns over time. In addition to real-time analysis, the system will also perform post-transaction fraud analysis based on a complete picture of activity across all payment service providers in the DS system and generate statistics on misuse risks.

Questions – Central Fraud Monitoring System:

4. A central fraud monitoring system could, on one hand, reduce the incidence of fraud within the digital shekel system, but on the other hand, it might challenge certain aspects of the DS privacy model. Do you believe it is important to establish a central fraud monitoring system, or can fraud monitoring be effectively conducted in a

decentralised manner by each participant in the system (as is customary in current systems)?

5. Is it important for such a system to operate independently of the Bank of Israel? What possible models exist for the operation of such a system?

3.3. Participants (ASPs, PSPs, and FIs)

In the digital shekel system, several types of "system participants". The system manager will define and enforce rules for connecting participants, as well as establish licensing processes for each participant.

1. **Digital Shekel Payment Service Providers** (hereinafter DS PSP or simply PSP) are essential entities in the system – without engaging with a payment service provider, end users will not be able to operate in the digital shekel system.
2. **Funding Institutions** are financial entities that manage payment accounts for the public outside the digital shekel system. Their participation in the DS system is required to ensure the ability to convert between DS and other forms of money – account balances or cash.
3. **Additional Service Providers** can offer optional services to end users, provide advanced services, support specific payment applications, and more.

Different entities can choose how to participate in the digital shekel ecosystem – as a PSP only, as an FI only (assuming they manage payment accounts for the public), as an entity operating both as an FI and an ASP, and so on. The system manager will define and enforce rules for connecting participants to the system, and from a technological standpoint, the system will support the ability to connect each participant and grant them the appropriate permissions to perform various activities, according to the participant type.[16] The regulatory framework (legislation, system rules, etc.) will ultimately define the conditions for the

[16] For example, in an API-based system like the one examined in the "Digital Shekel Challenge," PSPs would have permissions for the APIs required to open and close wallets and to perform payment actions, while ASPs would have permissions for the APIs needed to release locked funds in advanced payment applications. This is just an illustrative example.

activity of each type of participant (for example, legislation or regulation may stipulate that commercial banks of a certain size must also serve as PSPs). In any case, the regulatory hierarchy is expected to be such that FIs will be subject to the strictest regulation – because they hold public funds. This strict regulation already applies to them today, regardless of their future activity in the digital shekel system. The regulation on PSPs is expected to be more lenient – while they will be subject to rules from the realms of "know your customer," anti-money laundering and combating the financing of terrorism,[17] consumer protection,[18] and information and cyber security,[19] they will not hold customer funds, and therefore do not pose the financial risk associated with that. The lowest level of regulation will apply to ASPs. These entities are expected to be exempt (in most cases) from "know your customer" obligations since they are not the ones enrolling the end user into the system. In any case, every system participant will need to obtain a license, be supervised by a designated regulator, and meet the access requirements defined by the system manager.

Questions – System Participants:

6. Does the structure of three types of system participants (PSP, FI, ASP) adequately address the needs of the system and its users? Is the distinction between these types appropriate? Are additional types of participants necessary?
7. What should be the regulatory requirements for the different system participants?

3.3.1. PSPs

End users cannot connect directly to the digital shekel system but must do so through a PSP, which will handle the identification process and the opening of a digital shekel wallet for them. Three service package types that a PSP must provide will be defined: basic, advanced, and commercial. PSPs can offer services to the general public or specialise in certain user segments. Rules for reasonable refusal to provide service will be established. PSPs will have several potential sources of income.

[17] Chapter 7.4.
[18] Chapter 0.
[19] Chapter 7.5.

A PSP is an essential participant from the perspective of any end user, as there is no way to connect to the digital shekel system without engaging with a PSP. The digital shekel will operate within a two-tier model – while the digital shekel is a liability of the Bank of Israel to the end user holding it, end users will not have a direct interface with the Bank of Israel, but only with the PSPs – the payment service providers. It should be emphasised that at no stage do PSPs hold the end user's funds (this configuration was examined in "Project Sela").[20] A digital shekel in the hands of the end user is always a financial liability of the Bank of Israel to the user, not of the PSP.

The digital shekel system will also support a model of an indirect PSP – an entity that provides end users with all the services that a PSP provides but is not directly connected technologically to the system, rather it provides the services based on the technological connection of another PSP.

PSPs will perform all the necessary processes for end users – technological, business, and regulatory. They will handle the onboarding process of the end user to the system after a "know your customer" process, provide the end user with access technology (app, website, POS, smart card, etc., according to the standards defined by the system manager, see section 4.2), transmit payment commands to the system on behalf of end users, support wallet funding/defunding processes, provide customer service, and more.

PSPs will have several potential sources of income.[21] One of these sources will be charging fees according to established rules, and for this purpose, the system will technologically support their ability to automatically charge fees from end users as part of the payment process. Private end users will not pay fees for basic payment activities (these will be part of the free basic package, as described in Box 1), so a mechanism for an interchange fee payment in every merchant transaction will need to be established; the PSP of the merchant

[20] Bank for International Settlements, Bank of Israel, & Hong Kong Monetary Authority. (2023). An accessible and secure retail CBDC ecosystem: Project Sela.

[21] See further in this section for details on the service baskets that a PSP will be required to provide for free and for a fee, and additional services for which they can charge a fee. See also section 7.2 "Cost of Using the digital shekel."

will transfer part of the merchant fee to the PSP of the payer, and the system will need to support this technologically as well.[22]

To increase the ability of PSPs to develop a sustainable business model, they will not be required to onboard every end user who approaches them but will be allowed to specialise in certain user segments. Specialisation will allow PSPs to focus on developing solutions suitable for the sector in which they specialise, establish a business model with cross-subsidisation of activities from other areas they operate in, and reduce the cost and complexity of meeting "know your customer" obligations. Primarily, PSPs will be able to decide whether they choose to serve the private user sector, the business and organisational sector, or both. This choice will be recorded in the backend databases as it will be essential, for example, for the operation of fee collection mechanisms. Additionally, PSPs will be able to specialise in sub-sectors. For example, within the private user sector, a PSP could choose to specialise in members of a certain consumer club, a certain age group, etc. Within the business and organisational sector, a PSP could choose to serve only businesses from a certain industry (e.g., catering or transportation businesses), and so on.

One area where specialisation may be reflected is the types of access technology that the PSP will provide to its end users. Thus, a PSP serving only private users may not need to offer the option of receiving payments via POS, whereas a PSP serving only businesses may not need to offer a mobile app. The digital shekel will operate on the principle of universality, whereby any end user can pay and receive payment from any other end user, regardless of the identity of the PSP of that user or the type of access technology the user employs.[23]

Refusal to serve a customer must comply with regulatory provisions and not allow unreasonable refusal, particularly discrimination based on religion, race, gender, etc. Any end user eligible to connect to the digital shekel system will be able to do so.[24] As a result of allowing specialisation, there may be situations where some end users find that no PSP is willing to serve them. The Bank of Israel will monitor the participation rates of the public in

[22] For example, through a technological mechanism that initiates an automatic payment from the business to its PSP and from there to the payer's PSP as a result of each end user's payment transaction to a business.
[23] For further details, see section 4.2 "Access technology."
[24] See section 3.4.1 on "End Users".

the digital shekel system and the extent to which the digital shekel system is inclusive to different segments of end users. If the market develops in such a way that there is a concern that certain segments will be excluded, options for a "default PSP" will be considered, which will be required to provide the mandatory service package to any **Israeli resident** end user who wishes to receive the service.

In the digital shekel system, three packages of service types that a PSP must provide will be defined: basic, advanced, and commercial (for a PSP serving merchants). The basic package will be available to private end users (or those who do not meet the definition of a "commercial user") for free. The advanced package will be available to the same group of users and will include services that a PSP must offer but may charge for. The commercial package will include services suitable for merchants that receive regular payments in DS, and a PSP may charge for them.[25] Additionally, PSPs are expected to offer their customers a variety of advanced and other services that are not part of the packages defined by the system manager, and for these services, they can charge a fee.

A condition set by the system manager will be that the advanced and unique services offered by the PSP to its customers alone using the access technology it provides them will not harm the principle of universality towards customers of another PSP. For example, if the mandatory package does not include a deferred payment service, and the PSP chooses to provide it, its customers will be able to pay using this service to any end user in the DS, even if the user is a customer of another PSP or uses an access technology different from that provided by the first PSP to its customers. The principle of universality will also be maintained concerning system performance; the system manager will set performance requirements for PSPs regarding the basic transactions, and the obligation to meet these requirements will be regardless of the identity of the PSP on the other side of the payment transaction. Additionally, the requirements will ensure that performance is not a differentiating factor between PSPs, and competition between them will focus on additional advanced services.

[25] For further details, see section 7.2 "Cost of Using the Digital Shekel."

Box 1: Services that PSPs Must Offer to End-Users, and Fees They Can Charge

In designing the ecosystem and rules of the Digital Shekel system, there is an inherent tension between its nature as a public good of the Bank of Israel and the need to allow participants to maintain a profitable business model. As a public good, the aim should be for the usage costs to be negligible (similar to cash), but to achieve continuous innovation and high-quality service for users, it is necessary to have a many participants in the system, which will only happen if there is a business model that generates profitability.

In the user experience of digital means of payments Israelis are used to, private end users are generally accustomed to not having to pay variable fees for making payments, and sometimes they pay a relatively low fixed fee (e.g., monthly usage fees for a debit or credit card). In contrast, business users, particularly merchants receiving payments from retail customers, are accustomed to paying a fee for each transaction (e.g., merchant fee for card payments). The tension described above, on the one hand, and the usage habits of Israelis, on the other hand, necessitate defining the mandatory service package that a PSP will offer its customers. As seen below shows a division of this package into three packages: basic (free), advanced (for a fee), and commercial (for a fee). The basic and advanced packages will serve private users and businesses that do not receive retail payments, and the commercial package will serve merchants that receive retail payments.

Table 1: Mandatory Service Package that the PSP will offer to its customers:

	Payments Management	**Liquidity Management**	**User Management**	**Package Level**	
For a commercial user – fee can be	Initiating, approving and executing payments	Funding a wallet with digital shekels	Onboarding the digital shekel system	Basic - Free	For a non-commercial user

charged to all services	AML checks	Converting digital shekels to cash	Receiving access technology		
			User interface transaction history		
			Customer service		
	Automatic Payments	Waterfall/ Reverse waterfall	Cross border payments	Advanced – with a fee	
	Batch payments		Business user interface	Commercial – with a fee	

The table demonstrates that a variety of services that enable basic use of the DS will be provided for free, while for more sophisticated services, which the PSP will also be required to offer, it will be allowed to charge a fee.

It is possible that a certain service will appear on more than one level, depending on the service level: for example, PSPs may be allowed to offer a basic level of consumer protection for free up to a certain threshold of transactions or balance, and beyond this level, since the PSP's exposure to potential indemnification for fraud or misuse increases, it will be allowed to charge a fee for consumer protection. A business user operating commercially on the digital shekel will receive services tailored to this activity, for which the PSP will be allowed to charge a fee.

It should be emphasised that the table only represents examples, and the system rules that will be developed will include a wide range of services in each of the different packages. In addition to the mandatory package, PSPs can of course also offer many additional services for a fee, such as advanced payments, budget management mechanisms, and more.

Questions – PSPs:

8. Is it appropriate to allow a PSP to specialise only in certain segments of end users, so that they are not required to serve every customer who approaches them? How would such specialisation reduce entry barriers for PSPs?
9. Is there a need for a default PSP? Under what conditions should the decision to implement it be made? What possible models exist for operating such an entity? Could it potentially harm the business model of PSPs?
10. Does the mandatory service package adequately address basic processes? What is missing?
11. Can participants develop a business model that covers the cost of the mandatory services they must provide for free?
12. Is it reasonable for all PSPs to meet the same performance requirements, regardless of their size, market share, etc.?
13. Is there a sustainable business model for the operation of a large number of PSPs in the digital shekel that would support competition in the payments market?

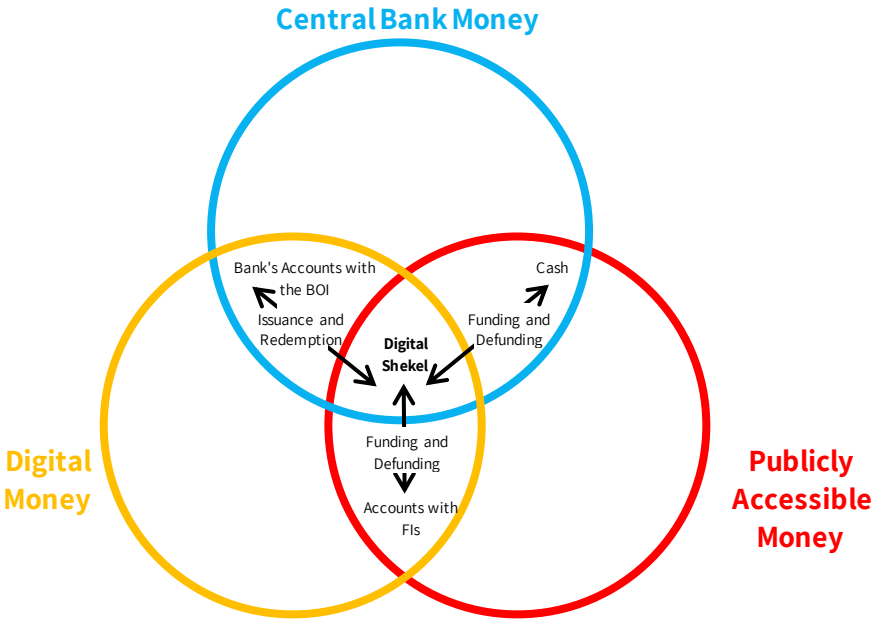
3.3.2. FIs

Financial institutions that manage payment accounts will be required, from a certain threshold, to participate in the digital shekel system as FIs and allow their customers to fund and defund their DS wallets against the account managed with them. An entity that manages payment accounts for its customers can serve as an FI even if it does not have an account in the RTGS system or a DS wallet, through an engagement with another FI. FIs will play a role in a universal solution for converting cash to digital shekels and vice versa.

As mentioned in section 2 above, the digital shekel will join other forms of money that already exist – cash (banknotes and coins), which together with the digital shekel and the banks' current accounts at the Bank of Israel constitute the "monetary base" (or "public money"), and the digital money deposited in the accounts of banks and payment companies (referred to as "private money"). To maintain the principle of "uniformity of money" – and

ensure that private shekels of any kind are always equal in value to public shekels of any kind, it is important that end users always have the ability to conveniently and efficiently convert between the different types of money. Financial institutions that manage payment accounts (Funding Institutions (FI)) will participate in the digital shekel system to allow end users to convert private money and cash to digital shekels. Converting another form of shekel to a digital shekel is a "funding" process, and the reverse process is "defunding" .[26]

Figure 3: Conversion processes between different types of money

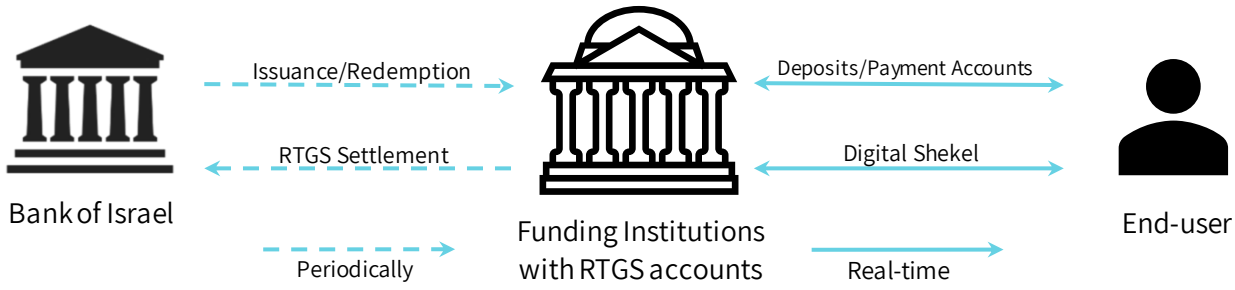


As a general rule, an FI can be any regulated corporation that allows its customers to manage an account with it for payment purposes. The most prominent example is a commercial bank that manages current accounts. Other examples include the Postal Bank, credit unions, companies licensed to provide financial asset services that offer payment account services, and so on. A corporation that serves as an FI will be required to allow its customers to fund their DS wallet from the account it manages for them and defund the wallet into the account, as described below. The regulatory framework will set thresholds or characteristics to determine which payment account managers will be required to serve as FIs in the system – for example, based on criteria such as the number of customers, market share, etc.

[26] For details on the funding and defunding process from the end user's perspective, see section 4.1 "Funding the Wallet."

Funding and defunding processes by customers of an FI holding an account at the Bank of Israel RTGS system, will be carried out against a digital shekel wallet held by each FI. Funding The FI's wallet will be reflected by debiting the FI's account in the RTGS system by the same amount, and defunding the wallet will be reflected by crediting this account (Figure 4). Funding and defunding the FI's DS wallet, in this case, are essentially actions of Issuance/Redemption of DS by the Bank of Israel. The DS system will support connectivity to the RTGS system, as well as automatic liquidity management for the FI; for example, an automatic issuance process to the DS wallet will be established when the balance in the wallet falls below a certain threshold defined by the FI, or alternatively, an automatic increase of the balance towards the end of the RTGS system's operating hours (to ensure that the DS balance in the FI's wallet is sufficient for customer funding needs when the RTGS system is closed), and so on.

Figure 4: Issuance and Redemption of digital shekels against a Balance in the RTGS System, and Funding and Defunding against a Balance in an FI



An entity that manages accounts for its customers can serve as an FI even if it does not have an account in the RTGS system,[27] or does not have a DS wallet.[28] In such a case, the FI will need to receive services from another FI and rely on the DS wallet and/or the RTGS system account of the other FI. A customer's funding or defunding will be reflected by debiting or

[27] In recent years, the Bank of Israel has allowed various entities that are not banks to connect to the RTGS system. Not all entities necessarily wish to connect or meet the required conditions to connect.

[28] Holding a DS wallet should not constitute a significant technological burden. However, an entity managing payment accounts may prefer not to hold such a wallet for liquidity management reasons, or holding restrictions policies may prevent it from holding a sufficient balance for its customers' funding needs.

crediting the account of the FI serving the customer, at the other FI. The scheme rules will define the conditions under which an FI directly connected to the DS system and the RTGS system will need to offer the required functionality to other financial entities so that they can also function as FIs and allow their customers to fund and defund their DS wallets.

FIs will play a role in a universal solution for converting cash to digital shekels and vice versa – funding and defunding a DS wallet against cash. Further details on this topic can be found in section 4.3.2.

Questions – FIs:

14. Is it appropriate to require all financial institutions that manage payment accounts for the public to participate in the digital shekel system as FIs, supporting the conversion of DS against payment account balances and/or cash? If not, what criteria should determine which institutions are required to participate?
15. Should entities connected to the RTGS system be required to allow other entities to operate as FIs based on their connection? What rules are necessary to facilitate this?

3.3.3. ASPs

ASPs will offer additional services on the digital shekel system. An ASP will only have access to some of the functionalities available to a PSP. An ASP will not be able to initiate a payment transaction in the end user's wallet. A PSP can also serve as an ASP.

The ability to offer services in the digital shekel system will also be granted to entities that do not wish to operate as PSPs. An Additional services provider will be able to offer various services such as budget management, analytics, advanced payment applications (such as conditional payments, etc.), and charge fees for these services. To offer these services, an ASP will have direct access to operate on the backend layer, for example, to read the balance in an end user's wallet, release money locked in one user's wallet for another user if the condition for the payment is met, and so on. This access will be conditional on authorisation by the end user, whether one-time, temporary, or ongoing. While all functionalities available to an ASP will also be available to a PSP (i.e., a PSP can function as an ASP), an ASP will have

access only to some of the functionalities available to a PSP. For example, an ASP will not be able to onboard an end user to the DS system and, in any case, will not be able to initiate a payment out of the end user's wallet, except through the PSP.

Questions – ASPs:

16. What types of services can an ASP offer to end users within the digital shekel system?

3.4. End-Users

The digital shekel system will support a wide range of end users. Different rules will be established for different types of users. The digital shekel will be a multipurpose digital currency that caters to retail users such as households and businesses, government entities, and wholesale users such as financial institutions. An end user of the digital shekel does not need to have a bank account, and the ability to perform any activity with the digital shekel – except for funding from an account – is not dependent on the existence of such an account. The PSP will conduct a "know your customer" process for the end user as part of the onboarding process.

The digital shekel system is designed to serve end users – individuals and organisations (businesses, non-profits, government entities, etc.) who can hold balances in digital shekel wallets and perform payment transactions between them. An end user of the digital shekel does not need to have a bank account or an account with any FI.

Questions – End Users:

17. What business and technological complexities might arise from the fact that a wide range of end users – individuals, small and large businesses, financial institutions, etc. – can operate within the digital shekel system?

3.4.1. General - Adults and Corporations

Any Israeli entity – an individual who is a resident of Israel,[29] a company incorporated in Israel, a non-profit organisation, etc., is eligible to be an end user and hold a digital shekel wallet. The necessary condition for this is the ability to undergo a "know your customer" procedure by a PSP. The government, through its various entities, will also be an end user and hold digital shekel wallet(s). Participants in the system may also hold a wallet and operate as end users – for example, as mentioned in section 3.3.2, entities serving as FIs will be required to hold a wallet[30] to support their customers' ability to fund and defund their wallets. As such, they can also operate as end users and perform transactions for themselves, make payments between them and other financial institutions, and between them and the Bank of Israel, including payments requiring final settlement (currently done in the RTGS system). Consequently, the digital shekel will also meet the common definition of a wholesale CBDC.

Box 2: Wholesale CBDC, Retail CBDC, and Multipurpose CBDC

In the CBDC literature and practice, a distinction is commonly made between two types of CBDC: wholesale (wCBDC) and retail (rCBDC). In fact, a wCBDC has existed in Israel and many other countries for many years[31] in the form of money in the current accounts of authorised entities in the RTGS system. In contrast, the idea of issuing an rCBDC – a central bank digital currency for retail use by the general public – is relatively new. Central banks began discussing it in the mid-2010s, partly in response to the emergence of cryptographic assets. These assets featured capabilities that were not present in most traditional payment systems, such as 24/7 availability, immediacy and finality, and the ability to perform "smart payments" based on the capabilities of these assets and the networks on which they operate. While, in its basic definition, all that is required for a financial asset to be characterised as a CBDC is that it constitutes a liquid digital liability of the central bank, regardless of the

[29] For minors, see section 3.4.2.
[30] Or operate through the wallet of another FI.
[31] Panetta, F. (2022). Demystifying wholesale central bank digital currency. *ECB Speeches*, *26*.. "There is a widespread misconception that wholesale CBDC does not yet exist. In fact, central bank money has been available in digital form for wholesale transactions between banks for decades. This misconception is fuelled by the commonly held assumption that wholesale CBDC needs to be operated using DLT. But wholesale CBDC is not synonymous with DLT, as it can be based on any digital technology."

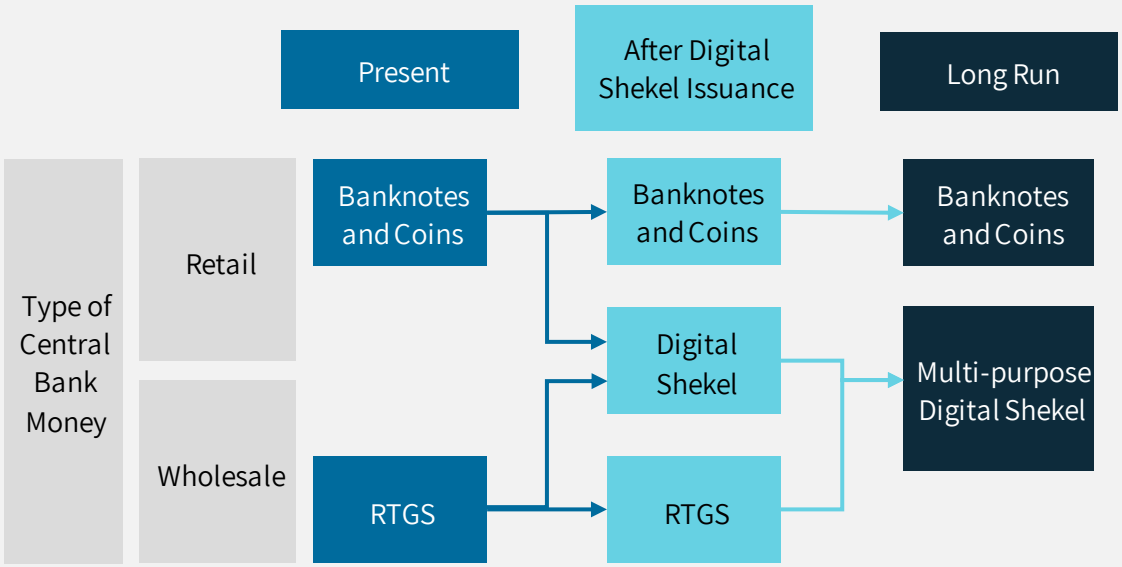
technology on which it is based, in professional discourse, the term CBDC has been associated not only with classic digital currency like that in bank accounts but primarily with a payment system characterised by technologies developed in the world of cryptographic assets. An rCBDC, being central bank money for use by the general public, is essentially the digital equivalent of physical cash. Hence, the idea of using smart money technologies as the equivalent of RTGS has been branded as "wholesale CBDC." So far, there is no consensus in the professional community regarding a clear definition of a wCBDC, its characteristics, and the technology on which it should be based, except for the statement that it constitutes a liquid digital liability of the central bank and that its user base is limited to financial entities (without a clear statement regarding exactly which entities other than banks).[32]

Since a wCBDC is fundamentally a technological improvement of an existing product, its establishment would be simpler, cheaper, and likely faster to implement than the establishment of an rCBDC, which raises technological, design, economic, monetary, legal, and even social issues, many of which are discussed and addressed in this document. Since financial and governmental entities, primarily commercial banks, will be required to hold digital shekel wallets and use them at least for funding and defunding DS wallets of their customers, by virtue of their role as, they will also be able to use these wallets for payments among themselves and with the Bank of Israel, and even to settle transactions arising from other payment systems, while benefiting from the finality of settlements in central bank money that currently takes place in the RTGS. This means that while there is a semantic separation between an rCBDC and a wCBDC, mainly due to the historical reasons described above, an rCBDC can, if properly designed, also function as a wCBDC. The DS will be a multipurpose digital currency ("multipurpose CBDC") that will address both the retail needs of end users such as households and businesses, and in this context, in particular, it can contribute to competition in the retail sector, as well as the wholesale needs of financial entities. Of course, different types of users will be subject to different rules and limitations, and there may be significant differences between retail and wholesale users and use cases. For example, private end users may be limited in the amounts they are allowed to hold in DS (see Chapter 7.6). On the other hand, they will enjoy privacy – especially vis-à-vis the central

[32] The BIS recently proposed the following distinction: "Wholesale CBDCs would serve a similar role as today's reserves or settlement balances held at central banks. However, wholesale CBDCs could allow financial institutions to access new functionalities enabled by tokenisation, such as composability and programmability." See footnote 1.

bank – regarding the balance in the wallet and the payment transactions they make (see Chapter 7.1). In contrast, commercial banks or government entities are not supposed to be limited in the amount of money they are allowed to hold at the central bank, and the central bank has full transparency regarding their activities, as is currently the case in the RTGS system. These differences will be defined at the user and wallet level, but the system will be the same system. The money used for grocery shopping and the money used for settling complex financial transactions will be the same money. This feature will save the need to deal with liquidity management challenges that may arise from recording central bank money in several separate systems.

Figure 5: Types of central bank money before and after the issuance of a digital shekel



Box 3: The Importance of a Wide Range of End-Users

Just as the use of shekels in cash is possible and permitted for everyone – any individual or corporation, in Israel and worldwide – optimally, the digital shekel should also be available to all users and allow any legal use. However, there may be various reasons to restrict the ability of certain individuals or corporations to use the digital shekel. For example, considerations of banking system stability may necessitate limiting the holding of digital shekels, as described in section 7.6. Anti-money laundering and counter-terrorism financing

considerations require ensuring that digital shekel users are identified and that its use is for legitimate purposes only.[33]

Beyond these considerations, the more users and types of users the digital shekel has, the better will the network effect ensure greater usability and benefit for users. For example, the more merchants that accept the digital shekel, the more worthwhile it will be for private users to hold and use it. The tendency of merchants to accept the digital shekel will increase if they are able use the money not only as a means of receiving payments from their customers but also as a means of payment to their suppliers or for paying salaries to their employees. Employees or suppliers who receive wages or compensation in digital shekels will want to pay with it, increasing the incentive for businesses to accept it, and so on. The presence of businesses among digital shekel users will also increase the feasibility of developing innovative and diverse use cases, as it is more challenging (and less economically viable) to develop innovative applications solely for the household sector, especially in a small economy like Israel. The government, through its various entities, is the largest payer and receiver of payments in the economy, and will play a significant role in creating the network effect that will ensure widespread adoption of the digital shekel if it allows the public to pay it in digital shekels (taxes, fees, fines, etc.) or receive payments from it in digital shekels (benefits, subsidies, grants, salaries, etc.). Additionally, the government could issue and redeem bonds and pay interest in digital shekels. The programmability of digital payments can support the development of a market for conditional payments against government permits or trading in assets requiring statutory digital registration (land registry at the Land Registry Office, vehicles at the Ministry of Transport, etc.). The design of the digital shekel takes into account a very wide range of users and use cases. However, it may be necessary to prioritise users and use cases in terms of the order they are developed and launched, and it may be necessary to postpone the development of some in the initial phase

[33] Additionally, monetary considerations may necessitate limiting the holding of digital shekels by non-residents. On one hand, there may be concerns about capital flight, but this is not relevant in Israel, where free capital movements already exist, especially given the ability to limit the digital shekel balance a user can hold. On the other hand, a G7 policy paper raised concerns that granting access to the CBDC of one country to the citizens of another country could create undesirable foreign exchange flows. This consideration also seems only slightly relevant to Israel, as the shekel is not a widely used currency in international trade, and it is unlikely that foreigners with no ties to the Israeli economy would want to use it widely.
Sunak, R., & Bailey, A. (2021). *Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs). G7 UK.*

to achieve a quick, safe, and stable launch (as explained in the introduction to this document). Over time, more users and uses of the digital shekel will be added, from different types and populations. The main limiting condition an end user to onboard the digital shekel system will be the ability of the end user to successfully undergo a "know your customer" process by a PSP willing to serve them.

3.4.2. Minors

There could be two models for the activity of minors in the digital shekel system. The first model is of a minor who holds a digital shekel wallet independently, and the balance in the wallet is their property. The minor has undergone a "know your customer" process, and the PSP has onboarded them to the system. The regulatory framework will define the age above which a minor can hold a wallet without parental or guardian consent, and the age range within which a minor can hold a wallet with such consent. Considering the digital shekel as a substitute for cash, it would be appropriate for these age ranges to be lower than those currently practiced for bank accounts.[34] The system will be designed to support the ability to identify a minor, onboard them to the system, and record and document the consent or withdrawal of consent by a parent or guardian at the relevant ages.

The second model is of a minor operating a wallet allocated to them by a parent,[35] as an indirect end user. The wallet would be owned by the minor's parent, but the parent would allow the minor to operate it. The parent would request the PSP to provide access technology for both the parent and the minor. The parent would need to report to the PSP who the indirect end user is so that the PSP can manage the various risks accordingly (fraud prevention, anti-money laundering, etc.) based on the expected usage profile of the wallet.

Questions – Minors:

[34] The Proper Conduct of Banking Business Directive 416 regarding minors' accounts states that any minor who is 14 years old is entitled to open a bank account provided that their parents or guardian have given written consent. A minor who is 15 years old and regularly receives wages transferred to their bank account may open a bank account without parental or guardian consent. Any minor who is 16 years old is entitled to open a bank account without the need for parental or guardian consent.
[35] For more on multiple wallets for an end user, see section 4.1 "End User Wallet."

18. Is it appropriate to allow minors to hold a wallet independently? Do the described models for such activity meet the need? What complexities might arise from this arrangement?

3.4.3. Foreigners

Foreign entities – corporations and individuals – will be allowed, but not necessarily entitled, to hold a digital shekel wallet. The condition for a foreigner to join as an end user in the digital shekel system is finding a PSP willing to conduct a "know your customer" process and enrol the user in the system. To enable this, the system will need to support the identification and registration of foreigners during the enrolment process. Foreigners – both individuals and corporations – will not be considered in the decision whether to offer a Default payment services provider solution (see section 3.3.1), and if such a solution is offered, foreign entities will not be eligible to benefit from its services. All rules and restrictions that apply to Israeli end users will also apply to foreign end users, and additional rules and restrictions may apply.

A specific case for foreigners that requires different consideration is tourists visiting Israel. For them, "know your customer" rules may be relaxed compared to other foreigners, allowing them to hold and operate a digital shekel wallet under unique limitations related to their period visitation. For this purpose, the system will be able to record relevant information to identify them as tourists.

Another specific case is foreign workers. As long as foreign workers reside in the Israel legally and under a permit, they are considered residents in the context of the digital shekel. Under specific conditions, asylum seekers and illegal residents may also be able to hold and use a digital shekel wallet, provided they can be identified and undergo a "know your customer" process.

Questions – Foreigners:

19. Is it appropriate to allow foreigners to operate within the digital shekel system? Are there additional complexities that arise from this that have not been described?

4. Basic User Journey in the Digital Shekel

An end user will be able to perform a variety of activities with the digital shekel through the system participants that serve them. Some are based on functionality provided by the backend layer, and some on functionality provided by the participants, primarily the PSP.

Questions – Basic User Journey:

20. Is there any additional basic functionality required in the digital shekel system that has not been described in this section?

4.1. Onboarding and Wallet Creation

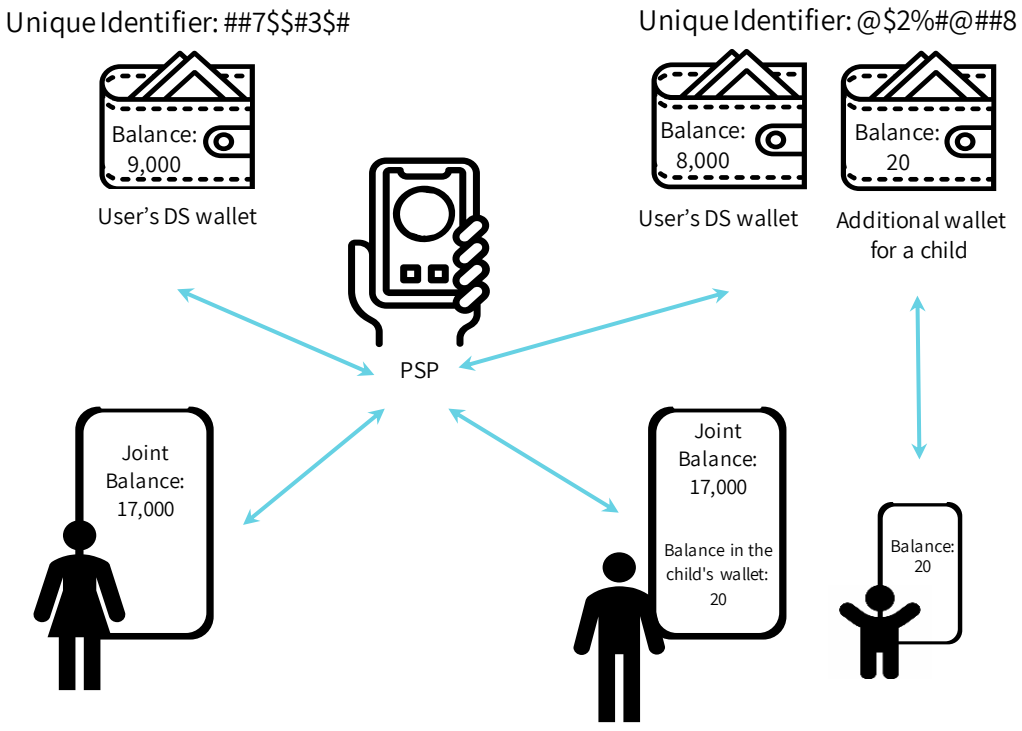
In the process of onboarding to the digital shekel system and opening a wallet, a unique identifier will be created for the end user, and an alias will be issued to them. A user can link multiple wallets to their unique identifier.

To operate in the digital shekel system, the end user must onboard it, and one or more wallets must be created for them.[36] When the user requests to onboard the system, they will contact the alias management system, which will request to issue a unique identifier for them in the main database[37] of the backend layer, to which the wallet created for the user will be linked. The system will issue the user an alias, and to complete the onboarding to the digital shekel system, the end user will contact a PSP (from a business perspective, the process may start with the end user contacting the PSP, who will assist the user in completing the process with the alias management system), which will conduct the "know your customer" process and approve the activation of the user's wallet(s).

[36] From a technological perspective, theoretically, an unlimited number of wallets can be linked to each identifier. There may be regulatory or system performance considerations that limit the number of wallets that can be linked to an identifier.
[37] See section 6.1.

A user can link multiple wallets to their unique identifier. These can be wallets that only they will operate (in such a case, they will need to define a default wallet for receiving payments, to which the user's alias will point), or wallets that they will allow an indirect end user (a child in the case of a family, a sub-unit in the case of an organisation/company, etc.) to operate (in which case, each wallet can have a different alias). In such a case, the primary user will need to report to the PSP who the indirect end user is so that the PSP can manage the various risks accordingly (fraud prevention, anti-money laundering, etc.) based on the expected usage profile of the wallet. A user can, but is not required to, link all their wallets to the same PSP – they can link each wallet to a different PSP, link one wallet to more than one PSP, and easily transfer a wallet with its balance to another PSP. Each wallet can be linked to only one unique identifier. PSPs can offer shared wallet functionality, for example, by jointly displaying the total balance in the wallets of a couple, etc (Figure 6).

Figure 6: Possible Architecture for the Functionality of a Shared Wallet for a Couple and an Additional Wallet for a Child



Questions – Onboarding to the Digital Shekel System:

21. What challenges might arise from linking an unlimited number of wallets to a single identifier? Should there be a limit on the number of wallets that can be opened for each identifier?
22. Is it important to allow an end user to enable access (both information and transactions) to their wallet(s) through more than one PSP? What challenges might arise from this?

4.2. Access technology

The digital shekel system will support various access technologies for funding and defunding the wallet and performing payment transactions. All online payments in the digital shekel system will be processed in the same manner, regardless of the type of access technology. The access technology will, as much as possible, allow end users to use devices they already have, so they do not need to acquire new hardware. The system manager will define rules and standards for new access technologies offered by the PSPs and a standard for a basic and accessible access technology.

To operate the wallet created for them, the user will receive one or more access technologies from the PSP – a hardware and/or software component that includes a secure container, and usually also a user interface (Figure7). The secure container will store the private keys that allow transactions to be performed from the end user's wallet. The system will support several types of secure containers: (1) a secure container installed in the edge device – that is, in the same device with the user interface (e.g., a smartphone); (2) a secure container located in the cloud; (3) a hybrid secure container that combines both. The user interface will allow the end user to view the balance, receive and make payments, and more. The digital shekel system will support at least the following four types of access technologies:

1. **Smartphones**, which will cater to most end users who are individuals.
2. **Smart cards, "stupid" phones, or other dedicated devices**, which will cater to parts of the public who cannot or do not wish to use a smartphone.
3. **Point of Sale (POS)**, which will cater to payments with merchants.

4. **Cloud-based interface (cloud API)**, which will cater to e-commerce, government payments, business-to-business payments, etc.

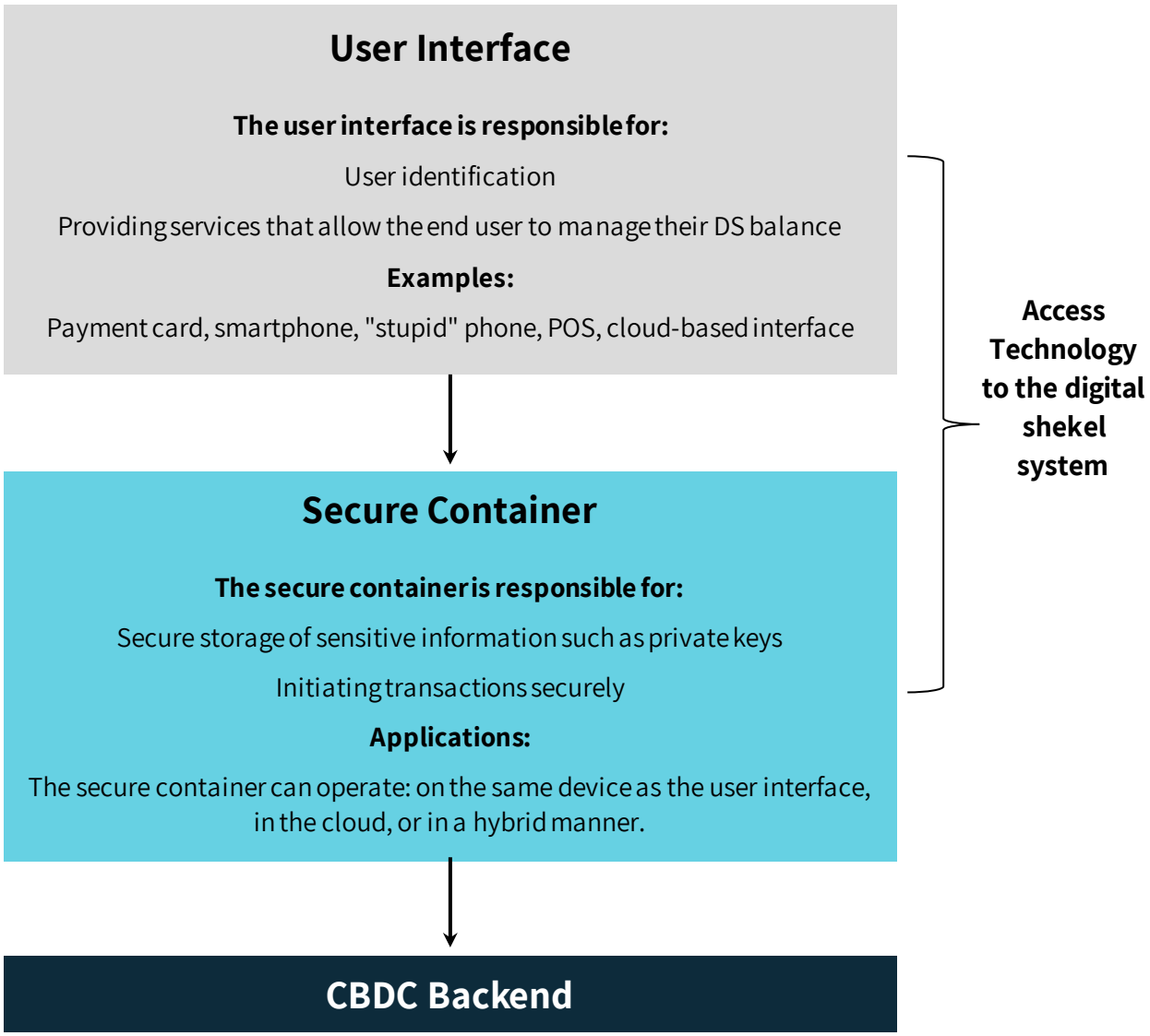
The backend layer will be indifferent to the type of access technology the end user uses, meaning all online payment transactions in the digital shekel system will be processed in the same manner, regardless of the type of access technology. Generally, transactions in the digital shekel can be performed between any two access technologies, of any type, in both Synchronous and Asynchronous manner. If a PSP wishes to offer an access technology where it is difficult to maintain this principle in synchronous transactions (for example, a PSP wants to offer an access technology in the form of a smart bracelet that does not interface with certain POS), the system manager will intervene, assist in finding a solution, and may decide to exempt the access technology from this principle if deemed appropriate.

The access technology will, as much as possible, allow end users to use existing payment devices they already have, so they do not need to acquire new hardware. This is particularly important in the context of POS, where emphasis will be placed on ensuring that existing POS systems also support connection to the digital shekel system. For this purpose, compatibility with the EMV protocol may be required. This will also ensure that the digital shekel access technologies are connected to the other operational systems of businesses, such as accounting, inventory management, etc.

Generally, the PSPs will develop the access technologies (themselves or by purchasing them from suppliers who develop them) and offer them to end users. The system manager will define rules and standards for the access technology offered by the PSPs. Additionally, the system manager will define a standard for a basic and accessible access technology,[38] which can meet the needs of people with disabilities, individuals whose digital literacy is insufficient to use access technology such as a smartphone, etc. Any PSP serving the private user sector will be required to provide this access technology to its users. If necessary, the subsidisation of this device by the Bank of Israel or other state authorities will be considered.

[38] The Bank of Canada coined the term "Universally Accessible Device" (UAD) in this context, see: Miedema, J., Minwalla, C., Warren, M., & Shah, D.(2020). *Designing a CBDC for universal access* (No. 2020-10). Bank of Canada.

Figure 7: Access Technology in the Digital Shekel System



Questions – Access technology:

23. What challenges might arise from the requirement that access technologies will allow end users to use their existing payment devices, so they do not need to acquire new hardware?

24. How should the access technology for the digital shekel be designed to be accessible to the entire public – including people of all ages, non-Hebrew speakers, those without a bank account, people with disabilities, and others?
25. Should every PSP be required to offer access technology and services that cater to all segments of the public described in the previous question? Should this requirement also apply to PSPs that exclusively serve businesses?

4.3. Funding the Wallet

An end user will be able to fund or defund the wallet against private money in a payment account they manage with an FI, or against cash.

Once the wallet has been activated and an access technology linked to it, the user can start operating it. Initially, they can receive payments or fund it. If the user wishes to fund the wallet, they can do so in two main ways.

Questions – Funding the Wallet

26. Are there additional mechanisms for funding and defunding a wallet, beyond those described in the section—such as funding and defunding against an account with a financial institution (FI) and cash—that should be enabled in the digital shekel system?

4.3.1. Funding the Wallet against an Account with an FI

An end user can link an account with an FI to their digital shekel wallet to fund and defund the wallet against debiting or crediting the account with the FI. Linking the wallet to an FI will also allow enable a "waterfall" or "reverse waterfall" mechanisms.

The end user can fund the wallet against private money in an account they manage with an FI – similar to how they can currently withdraw cash from said account. To do so, they will provide the PSP with the account details at the FI and request to link the account to their

digital shekel wallet. The PSP will forward the request to the FI, and after the FI verifies the user's identity and receives their approval to link the account to the wallet, the link will be established. Now, the end user can contact the PSP through the user interface provided and request to perform the funding. The PSP will send the request to the FI, which will perform two actions: 1) Transfer the requested amount of digital shekels from the FI's digital shekel wallet (see section 3.3.2) to the end user's digital shekel wallet. 2) As a complementary process, the FI will debit the user's account with the funding amount. If the user does not have sufficient balance in the account with the FI (or the transaction would bring the user's account below the overdraft limit allowed by the FI), the FI will reject the funding request, and the user will receive a notification in the PSP interface that the funding was not completed.

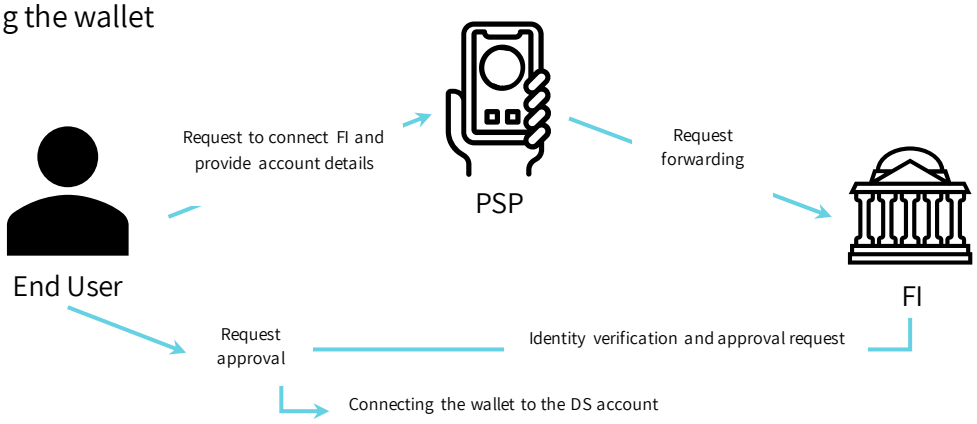
When the user has a positive balance in the wallet, they can defund the wallet, which is the reverse of the funding, by contacting the PSP, transferring digital shekels from the user's wallet to the FI's wallet, and crediting the user's account with the FI.

A specific case of defunding is called a "Waterfall" operation, and a specific case of a funding is called a "Reverse Waterfall". In a case where, following a payment received into the wallet, the balance exceeds the allowed balance according to the holding limit[39] (or a balance set by the user according to their preference), the waterfall mechanism will be activated, and an automatic defunding will be performed to bring the wallet balance back to the allowed balance. If the end user has not linked an FI account to their wallet or has chosen not to activate the waterfall mechanism, the balance cannot exceed the holding limit, and an incoming payment transaction that would result in such a situation will be rejected. Conversely, the user can predefine that if they wish to make a payment but the wallet balance is insufficient (or the payment would bring the wallet balance below a threshold set by the user), the reverse waterfall mechanism will be activated, automatically funding the wallet from the FI account with the required amount to complete the payment transaction.

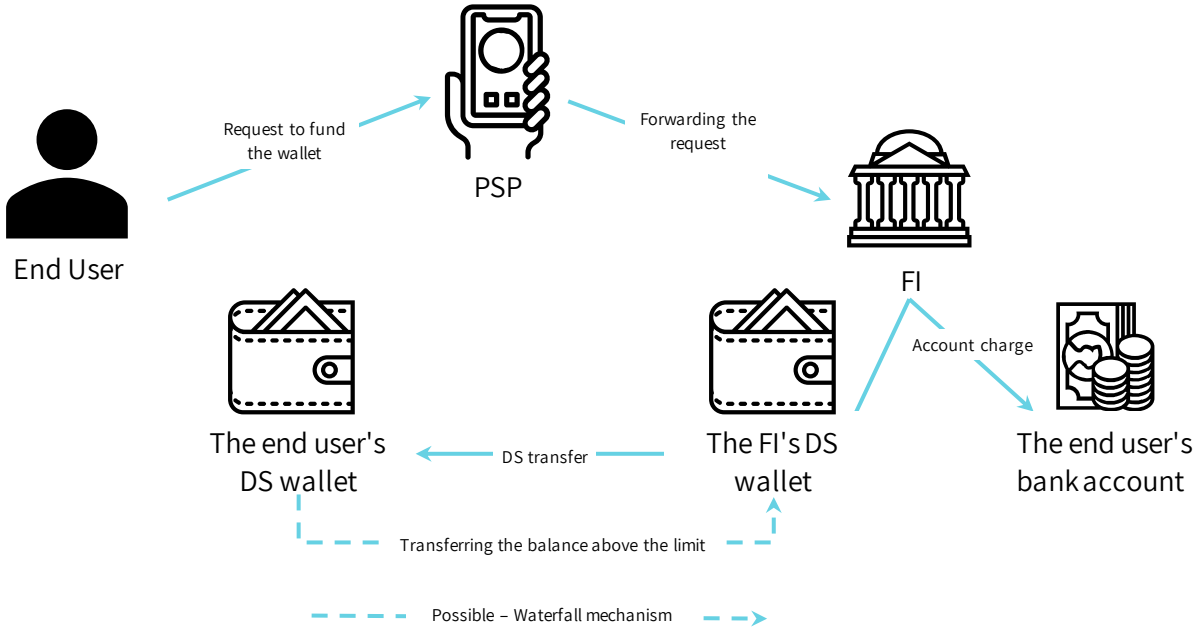
[39] See section 7.6.

Figure 8: Connecting a Wallet to an FI and Funding the Wallet

1. Connecting the wallet



2. Funding the wallet



Questions – Wallet Funding Against an Account with an FI:

27. What complexities might arise from the requirement to allow wallet funding and defunding against an account with an FI 24/7/365, including beyond regular banking business hours?
28. Should there be limits on the amount, frequency, or other variables regarding wallet funding and defunding by a user? For what reasons? Should these limits apply at the

system-wide level, or should each FI be allowed to set limits according to its own considerations and needs?

29. Should the waterfall and reverse waterfall mechanisms be implemented? What complexities might arise from these mechanisms?

4.3.2. Funding the Wallet against Cash

An end user will be able to fund or defund their digital shekel wallet against cash – at an ATM or FI service counters, even if they do not have an account with the FI. The responsibility for monitoring the funding and defunding processes against cash lies with the PSP and not with the ATM operator or the FI.

The digital shekel system will have a universal mechanism for funding and defunding the digital shekel wallet against cash. This mechanism will include the FIs, the national ATM switch, and a dedicated component in the backend layer at the Bank of Israel. The end user will contact the PSP through the user interface and request to defund or fund the wallet against cash for a certain amount. The PSP will perform the necessary checks to allow the transaction – ensuring sufficient balance, checks required by anti-money laundering rules regarding cash activities,[40] etc. After that, the PSP will issue the user a one-time code (or another identification means) and send a message to the ATM switch that includes the code, the user's wallet address to/from which the digital shekels should be transferred/received, and additional information such as the expiration time of the funding request.[41] The user will approach any ATM connected to the mechanism and present the code received from the PSP to the ATM. In the case of wallet funding, the user will insert the cash amount they requested into the ATM. As a result, a message will be sent from the ATM switch to the backend layer at the Bank of Israel, which will issue digital shekels from the central bank to the user's wallet, and simultaneously redeem digital shekels from the digital shekel wallet of the FI operating

[40] For more details, see section 7.4.

[41] No information about the end user's identity will be transferred – this will be retained only by the PSP.

the ATM the user approached.[42] In the case of wallet defunding, the user will receive cash from the ATM, thereby authorising the mechanism to redeem digital shekels from their wallet and issue them to the wallet of the FI operating the ATM.

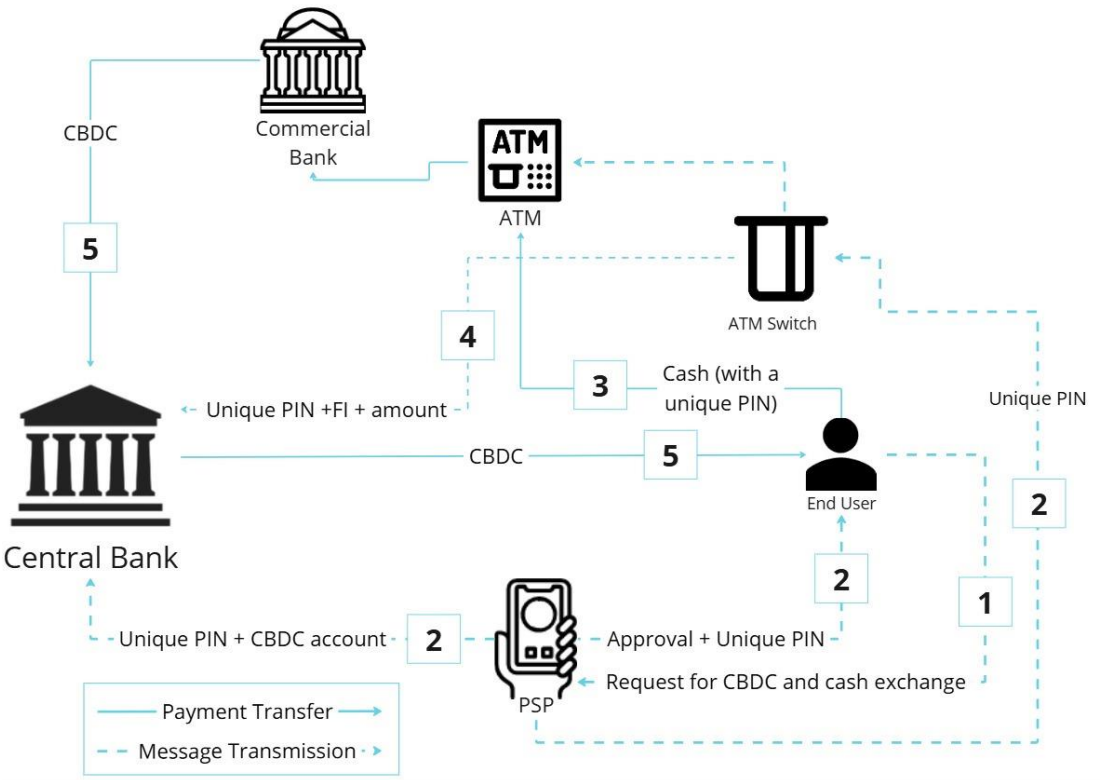
In the described mechanism, the Bank of Israel acts as an intermediary between the end user and the FI operating the ATM. The possibility of settling the transaction as a transfer of digital shekels between the FI and the end user without involving the Bank of Israel was considered, but this configuration could raise issues of privacy and (undesirable) obligations of the FI regarding anti-money laundering rules. In the described model, the responsibility for anti-money laundering aspects lies entirely with the PSP, which has a relationship and business engagement with the end user, and the user's privacy vis-à-vis the FI is not compromised.

If performing an issuance/redemption process for every cash-to-DS or vice versa conversion is operationally complex, additional practical solutions will be considered to maintain the separation principle between the FI and the end user, such as a temporary account managed by the central bank or the ATM switch operator.

As an alternative to an ATM, end users will be able to perform the cash funding and defunding as described above at the service counters of any FI, including one where the user does not have an account, as long as it has physical branches and provides cash services at the counter.

[42] The mechanism can also operate if the ATM operator is not an FI, provided it has an agreement with an FI for this purpose.

Figure 9: Wallet Funding or Defunding Process against Cash at an ATM



Questions – Wallet Funding Against Cash:

30. What challenges might ATM operators face if required to allow all digital shekel users to fund and defund cash against DS?
31. What other solutions can be considered for funding a digital shekel wallet at an ATM while maintaining anti-money laundering and counter-terrorism financing principles, as well as privacy principles?
32. What complexities might arise from the requirement that an FI allows cash funding and defunding at the counter for individuals who are not its customers?
33. What considerations should be taken into account when setting limits on the amounts for cash funding and defunding?

4.4. Online Payment Transactions

An online payment transaction can be performed between any two end users in the digital shekel system. Except in exceptional cases, a PSP cannot initiate a payment without explicit authorisation from the end user. The system will support micropayments as well as very high-value payments (e.g., wholesale payments).

A payment transaction in the digital shekel means reducing the balance in the payer's wallet while increasing the balance in the payee's wallet. A payment transaction can be an asynchronous – one where only the payer's user interface needs to be active, and no action is required of the payee's user interface for the transaction to proceed. Such a transaction does not require prior communication between the two end users. The paying end user will contact the PSP through the user interface, provide the alias or wallet address of the payee, and request to perform a payment for the specified amount to the payee. The payer's PSP will perform several necessary checks such as: (1) Ensuring sufficient balance – it will check that the end user's wallet has sufficient balance to perform the payment, and if not, that the payer has defined a reverse waterfall mechanism to fund the missing amount from their FI account; depending on the transaction characteristics, it may also check (2) Payee identity verification – the alias will be presented to the payer to ensure the payment is being transferred to the correct payee (confirmation of payee); (3) Compliance with anti-money laundering and counter-terrorism financing rules – ensuring the payment does not raise concerns of violating anti-money laundering rules; (4) Fraud monitoring – checking the payment against the fraud monitoring system. Based on the results of these checks, the PSP will either forward the payment request to the settlement engine or reject it. The payee's PSP will ensure that the payment opertion does not pose a risk of violating any rules and will also ensure that receiving the payment does not push the payee's balance above the allowed holding limit,[43] and if so, that the payee has defined a waterfall mechanism to receive funds into the wallet even if the balance exceeds the limit. If all these conditions are met, the payment will be executed, and the balances of both users will be updated immediately.[44]

[43] This check may be performed by the settlement engine, and the payee's PSP may not be required to perform it.
[44] See section 4.5 "Immediacy and Finality" for more details.

Both users will be able to receive a notification that the transaction was successfully completed, even though the payee did not actively participate in it.

Figure 10: The Basic User Journey in the Digital Shekel System

Although from the perspective of the settlement engine, the request to perform a payment transaction comes from the PSP, it should be emphasised that a PSP cannot initiate a payment without explicit authorisation from the end user. This feature will be enforced not only by the system's rules but also technically – for example, by requiring that a request to the settlement engine to perform a transaction from the wallet be authorised by the private key held solely by the end user. A technical solution will be provided for special situations where a transaction needs to be performed without the end user's authorisation – for example, to enforce judicial orders such as inheritance or seizure orders.[45]

A payment transaction can be a synchronous payment – where the user interfaces of both parties to the payment are involved, requiring communication between the two end users. A clear example of this is an RTP (request to pay) process, where the payee sends a message to the payer that includes at least the payee's wallet address, and in most cases, also the payment amount and additional information. The message can be transmitted between users by scanning a QR code, through a message between user interfaces via the PSPs, or any other way. The message from the payee appears in some form in the payer's user

[45] A possible solution is that to enforce a judicial order, both the private key of the court and that of the PSP would need to be presented to the settlement engine.

interface, allowing them to approve the transaction. After that, the payment proceeds like the asynchronous payment described above.

An asynchronous payment can be performed between any two end users, regardless of the type of access technology both users are using. This rule also applies to synchronous payments; however, there may be situations where the implementation is complex. For example, currently, not every point of sale (POS) can initiate a payment to an end user in the system. Another example is access technologies that are not equipped with a user interface – such as a smart card that allows an end user to operate in the digital shekel but does not have a user interface.[46] To avoid compromising the principle of universality of the digital shekel, the system manager will define cases where an access technology can be exempt from supporting synchronous transactions with other access technologies.

An online payment can be performed between any two end users in the digital shekel system. Specifically, if we define four main sectors of end users – private (P), businesses (B), financial entities (F), and government entities (G), then every combination of payment transactions between end users from all sectors will be supported by the digital shekel system (Table 2). The system will support very small and high-frequency payments – for example, payments of a hundredth of an agora at a frequency of several payments per second, for micropayment use cases, as well as very high-value payments (e.g., wholesale payments between financial entities).

[46] Similar to, for example, the Rav-Kav card.

Table 2 – Examples of Use Cases between End Users from Different Sectors, using the Digital Shekel

Payee / Payer	P	B	G	F
P	Sale of a second-hand product, transfer between family members	Purchase from a business	Tax payment, receiving government services through a government website	Loan repayment, monthly credit card balance payment [47]
B	Salary payment, customer refund	Payment to a wholesaler or raw material supplier	Payment of taxes, levies, licenses	Loan repayment, insurance premium
G	Salary payment, allowances	Government grants		Insurance premium, government bond coupons
F	Salary payment, insurance benefits	Supplier payments, acquirer payments by debit card to a business[48]	Tax payments, purchasing government bonds	Clearing payment transactions from other payment systems

Questions –Online Payment Transaction:

34. To what extent is it important to design the system so that a PSP cannot initiate a payment transaction without explicit authorisation from the end user for each transaction? What challenges might arise from this requirement in terms of user experience?

[47] As described in section 5.1.1.2.
[48] Ibid.

35. How can we ensure that the end user is the only one who can perform payment transactions from the wallet, while also accommodating special situations where a transaction needs to be performed without the end user's authorisation?
36. Is it important for the digital shekel to support use cases between any two end users, regardless of type (as described in Table 2)? What challenges might arise from this?
37. What challenges might arise from the digital shekel system supporting both very small and very large payments?

4.5. Immediacy and Finality

Every transaction in the digital shekel will be immediate and final, with finality embedded both in the system design and from a legal perspective. Every funding process will be immediate and final, both in the digital shekel wallet and in the user's account with the FI. The system will be available to process payment, funding, and defunding transactions 24/7/365.

Every payment transaction in the digital shekel – whether online (see section 4.4) or offline (see section 5.3) – will be immediate and final. Once all conditions for performing the transaction are met (balance check, anti-money laundering controls, fraud prevention controls, etc.), the time it takes for the balances of the payer and the payee to be updated and for the transferred amount to be available for the payee to use will not exceed a few seconds.[49] This will be true regardless of when the transaction is performed – the system will be available and process payment transactions 24/7/365.[50] Funding processes will also be immediate – both the digital shekel wallet and the user's account with the FI will be updated immediately after the funding, and the updated balance will be available for use both in the digital shekel wallet and in the account with the FI.

[49] Such immediacy is commonly referred to as T+0.

[50] For system performance reasons, payment transactions can be scheduled for times with lower transaction volumes, as described in section 6.3.

The finality of payments in the digital shekel will be embedded both in the system design and from a legal perspective. The system design will ensure that balance updates following a payment transaction are irreversible – the only way to cancel a payment transaction is to initiate a transaction in the reverse direction.[51] The fact that end users are not defined as participants in the system allows for legal embedding of finality as well. For this purpose, the digital shekel system will be defined as a "designated controlled payment system" under the Payment Systems Law.

The system will include functionality that allows, before an end user performs a payment transaction, to display a clarification that the payment they are about to perform is final and irreversible. The system rules will define for which types of users and transactions such a clarification must be displayed.

Box 4: The Meaning and Importance of Immediacy and Finality

The design of the digital shekel aims to combine the maximum advantages of both cash and digital money while minimising their disadvantages. One of the benefits of paying with central bank cash is that once the cash has changed hands (i.e., the payment has been made), the transfer is final, and the value is guaranteed, as it is a liability of the central bank. The main disadvantage of cash is the need for physical proximity of the payer and the payee, as well as the legal limit on the maximum amount allowed for payment transactions. The only digital alternative currently available to the public for immediate, final, and secure payments settled in central bank money is an RTGS transfer, but it involves high fees for small transfers, is not available 24/7, and in terms of user experience, the immediacy is sometimes reflected in minutes rather than seconds. One of the inherent advantages of the digital shekel is that it is central bank money that will enable immediate, final, and always-available payments at minimal to zero cost to the end user.

[51] In an account-based settlement engine, finality will be defined as the moment when the balances in the payer's and payee's accounts are updated following a payment transaction. In a token-based settlement engine (including UTXO), finality will be defined as the moment when the tokens are irreversibly deleted from the payer's wallet and are in the payee's wallet, making them available for the payee to use.

A survey conducted by the Currency Department of the Bank of Israel[52] found that for merchants, the prominent advantages of cash are liquidity and immediacy (respondents mentioned attributes such as "liquid," "available,", "money in hand," "immediate," "quick," "immediately visible") and finality ("secure," "reliable," "certain payment"). A survey conducted in the Eurozone,[53] commissioned by the ECB, also found that immediacy and the ability to quickly use the received money (finality) are critical attributes for business owners, as they facilitate cash flow management, and businesses are dissatisfied with existing means of payments in this regard.[54] The immediacy and finality also support the ability of the digital shekel to serve as a means of payment for transactions requiring conditional payments, such as Delivery vs. Payment or Payment vs. Payment (PvP/DvP – see section 5.2.1). However, it should be noted that immediacy and finality can be a disadvantage concerning consumer protection against errors and fraud – similar to cash. Part of the digital shekel's design is intended to mitigate these disadvantages as well (see section 07.3).

Questions – Immediacy and Finality:

38. Similar to cash payments, a payment transaction with the digital shekel is final and immediate – meaning it is irreversible. Is this an advantage or a disadvantage of the digital shekel from the user's perspective?
39. What challenges might arise from the requirement that funding and defunding processes be updated immediately 24/7/365 in the customer's account with the FI, including processes resulting from a waterfall or reverse waterfall mechanism? Could this pose a barrier to entities operating as FIs?

[52] Bank of Israel – Currency Department (2023), "Currency Department Review for the Years 2020-2022." (Link only available in Hebrew).
[53] Kantar Public, (2022) "Study on New Digital Means of payments".
[54] The summary of the business owners' focus group responses stated: "Instantaneity would therefore be the most relevant improvement and an essential driver for the adoption of the new means of payment".

5. Advanced User Journey in the Digital Shekel

The digital shekel system will be designed to support complex transactions and innovative payment use cases.

To ensure innovation, efficiency, and maximise the digital shekel system's contribution to the payment ecosystem and the economy as a whole, the digital shekel will enable complex transactions and support innovative use cases. Some of the capabilities detailed in this chapter are already present in other digital means of payments, and the digital shekel will incorporate them to ensure it is not inferior to existing solutions. Additionally, the digital shekel will introduce new capabilities that do not currently exist, setting it apart from other means of payments. A crucial aspect in this context is the interoperability of the digital shekel with other payment systems, which will ensure a seamless user experience and overall system efficiency.

Questions – Advanced User Journey:

40. This chapter describes advanced functionalities of the digital shekel system. Are there additional advanced functionalities that should be included but are not mentioned in this chapter?

5.1. Interoperability

The digital shekel system will be interoperable with other payment systems domestically and internationally, with regulated digital asset systems, as well as with relevant national information systems and infrastructures.

Interoperability is the technical, semantic, and business compatibility that allows the system to be used in conjunction with other systems.[55] In the context of payment systems,

[55] Bank for International Settlements, & Group of Central Banks. (2021). CBDCs: System design and interoperability.

interoperability can be thought of as a framework that allows a payment to be made using one means of payment/payment system and received using another means of payment/payment system easily, with minimal friction, human intervention, cost, and time. Another aspect is the ability to link additional processes in databases and data systems that are not part of the payment system to the payment transaction.

The digital shekel will maintain interoperability across four main dimensions – with other payment systems in Israel, with payment systems abroad, with regulated digital asset systems, and with relevant national information systems and infrastructures.

5.1.1. Local Payment Systems

As described in section 3.3.2 the issuance/redemption of digital shekels will be reflected in a debit/credit of an FI account in the RTGS system. This conversion will require a link between the RTGS and the digital shekel system. This link will need to be automatic, allowing each system to write or send commands to the other. Funding and defunding a digital shekel wallet against cash will require connectivity between the digital shekel and the ATM switch, as described in section 4.3.2. These are examples of the digital shekel's interoperability with local payment systems in the context of issuance/redemption and funding/defunding. Later in this section, we will describe interoperability processes with other payment systems designed to facilitate transactions where one leg is in digital shekels and the other in a different payment system.

5.1.1.1. Payment Accounts and the MASAV System

The system will support the ability to make payments from a digital shekel wallet to a payment account at a bank (or another entity, such as an FI managing payment accounts), and vice versa. For example, an end user will be able to transfer funds from their digital shekel wallet to another party's bank account, even if the other party does not have a digital shekel wallet. In the opposite direction, it will be possible to transfer funds from a bank account to a digital shekel wallet, even if the account holder does not have a digital shekel wallet. This functionality can be supported in two ways:

1. **Direct Transfer from a Digital Shekel Wallet to a Bank Account**: An end user will contact the PSP through the user interface and request a transfer to a bank account by entering the account details. The transfer will be reflected in a payment transaction from the end user's digital shekel wallet to the bank's digital shekel wallet managing the payee's account, with the payment message indicating the payee's account number at that bank. The bank will receive the digital shekels into its wallet and credit the payee's bank account. This process is similar to a customer depositing cash directly into another customer's account. If the bank cannot complete the transfer, for example, because the account details provided by the user to the PSP are incorrect, the bank will return the digital shekels to the paying end user. In the opposite direction, a bank customer will request a transfer and enter the payee's digital shekel wallet details. The bank will debit the customer's account and transfer the funds to the payee's digital shekel wallet. In both directions, the digital shekel system also serves as the messaging system, instructing the bank on which account to credit or debit and to which digital shekel wallet to transfer the funds.
2. **Transfer via MASAV**: MASAV[56] can serve as an orchestrator of transfers between digital shekel wallets and bank accounts and vice versa provided that dedicated connectivity is established between the two systems. In this scenario, when the user contacts the PSP to initiate the transfer, the payment order from the user's wallet to the bank's digital shekel wallet will first be sent to MASAV, which will then request to lock the amount in the payer's wallet for the bank. MASAV will send the payment message to the bank, and after the bank verifies that the message is correct and that it is able to credit the payee's account, the lock will be released, the amount will be transferred to the bank's wallet, and the bank will credit the customer's account. In the opposite direction, the payment message to the bank will pass through MASAV, but there is no need for a lock, as the digital shekel system will not permit a transfer from the bank's wallet if the payee's digital shekel wallet does not exist. For this purpose, MASAV must be an ASP in the system or utilise the services of another ASP.

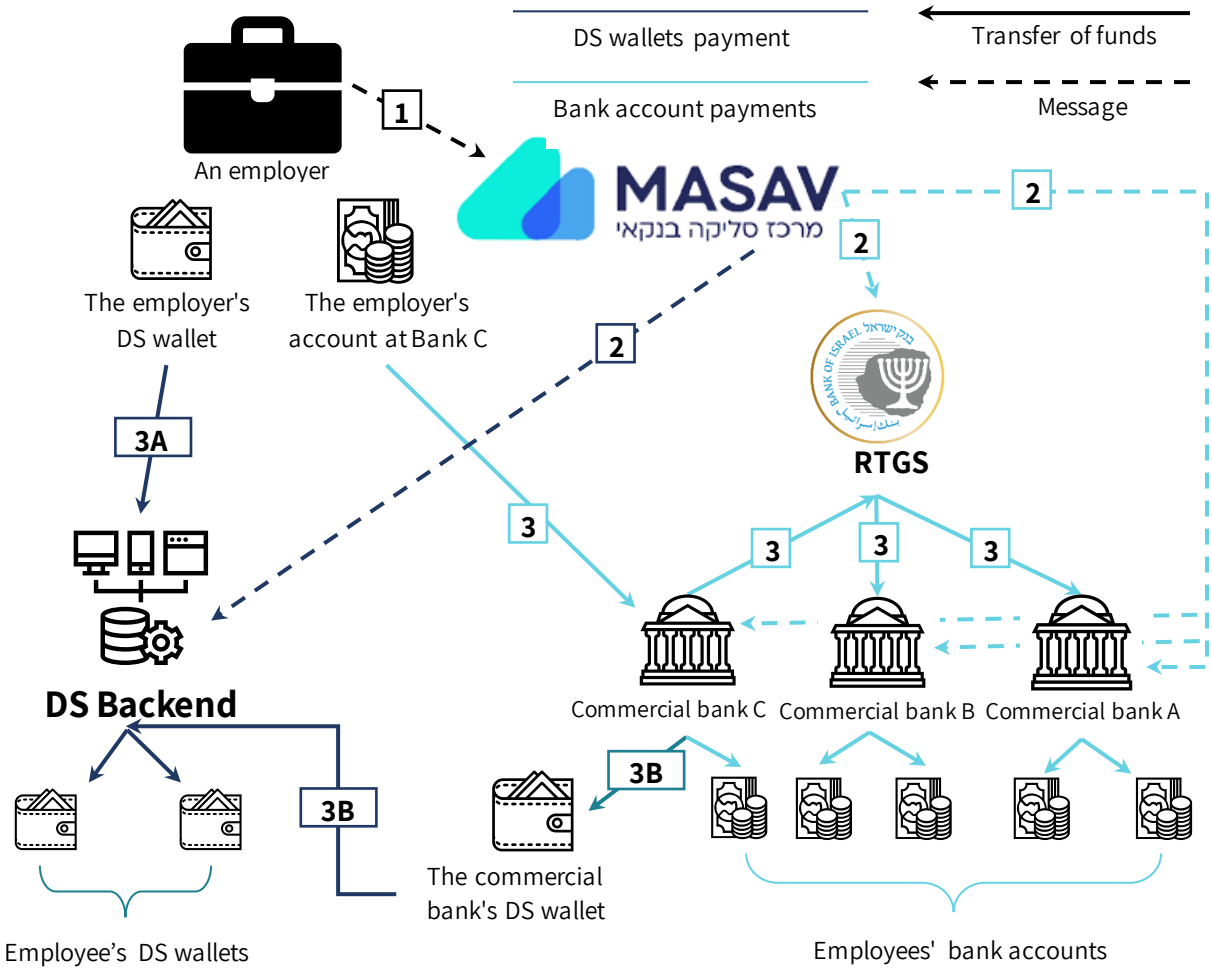
[56] MASAV (Hebrew acronym for "Bank Clearing Center" operates Israel's Automated Clearing House and Faster Payments.

To enable these processes, the user interfaces offered by the PSPs should include the option to request a transfer to a bank account and allow entry of account details. Similarly, the user interfaces of the banks should include the option to transfer funds to a digital shekel wallet and allow the entry of the wallet's alias. The digital shekel will receive an identification code within the payment system,[57] ensuring that the existing interface at the banks – based on the payment institution's identification code and account details or account alias – will be able to support these payments in their existing format.

A special case of transfer between bank accounts and digital shekel wallets and vice versa is batch payments. MASAV allows various entities to make payments to a large number of payees – for example, salary and pension payments, supplier payments, and more. Special connectivity between the digital shekel system and MASAV will allow splitting these payments also to the payees' digital shekel wallets. For example, an employer paying salaries to employees' bank accounts or digital shekel wallets according to their choice through the MASAV batch payment system will be able to enter the digital shekel wallet details of their employees into the system. MASAV will manage the transfer of funds from the employer's bank account to the employees' bank accounts who chose to continue receiving their salary in the bank account, and simultaneously – to the digital shekel wallets of those who chose to receive the salary in digital shekels. The transfer can be made from both the employer's bank account and the employer's digital shekel wallet. This applies not only to salary payments but also to any other type of batch payments. For hybrid batch collection (debits of both bank accounts and digital shekel wallets), for example, a utility company's collection from its customers, MASAV will need to receive authorisation from end users to debit their digital shekel wallets in some form.

[57] The identification code will be for the entire digital shekel system, allowing transfers to any wallet in the system, regardless of the specific PSP's identity.

Figure 11: The Process of Batch Payments between Bank Accounts and Digital Shekel Wallets



1. In the first stage, the employer sends a message to MASAV detailing the amounts and destinations for the transfer (bank accounts and digital shekel wallets).
2. In the second stage, MASAV forwards the messages to the respective systems. For bank accounts, a message is sent to the RTGS system for interbank transfers, and another message is sent to the banks specifying which accounts to credit and debit. For digital shekel transfers, a message is sent to the digital shekel system indicating which wallets to credit and debit.
3. In the third stage, the debits and credits are executed. For transfers to bank accounts, the RTGS system performs the transfers between the commercial banks, which then transfer the funds to the accounts. For transfers to digital shekel wallets, the digital shekel system debits and credits the relevant wallets. If the employer chose to make the payment from their digital shekel wallet, a debit will be made from this wallet (3a). If the employer opts to debit their bank account, a debit will be made from the digital shekel wallet of the employer's commercial bank (Commercial Bank C), and the commercial bank will subsequently debit the employer's bank account for the corresponding amount.

5.1.1.2. Payment Cards

When a customer pays using a card,[58] the issuer of the card ultimately debits the customer's bank account. If a card is issued by a bank, the link between the card and the bank account is automatic; for a non-bank card, the customer signs an authorisation to debit the account in favour of the issuer. Digital shekel end users will have the option to debit their digital shekel wallet for their card payments instead of their bank account. This debit will be executed by transferring digital shekels from the end user's wallet to the issuer's wallet.[59]

When a merchant receives payments via a card,[60] the acquirer ultimately credits the merchant's bank account. Merchants will have the option to credit their digital shekel wallet instead of their bank account. The credit will be executed by transferring funds from the acquirer's digital shekel wallet (or bank account) to the Merchant's digital shekel wallet.

End users will also be able to load prepaid cards by transferring funds from their digital shekel wallet to the digital shekel wallet or bank account of the prepaid card issuer.

5.1.1.3. Checks

It will be possible to deposit physical checks into any digital shekel wallet instead of into a bank account. The PSP's user interface[61] will include an option to deposit a physical check by taking a photo of it, similar to current practices. At the end of each business day, the PSPs will transfer the check payments and a file containing the details of the wallets to be credited to the banks on which they are drawn and notify the customer. The banks will have three days, as usual, to transfer the money from their digital shekel wallet to the depositors' wallets, or send a notice of dishonour to the PSP, which will notify the user in the app about the returned check and the reason for it. The PSPs will allow both the deposit and withdrawal of digital checks against a digital shekel wallet. This functionality will be further specified after the overall specification of digital checks in Israel is finalised.

---

[58] "Credit card," meaning a deferred debit card, "debit card," meaning an immediate debit card. This paragraph does not refer to prepaid cards.

[59] Or to the issuer's bank account, similar to the transfer from a digital shekel wallet to a bank account described in section 5.1.1.1.

[60] This also applies to prepaid cards.

[61] This functionality is trivial when the user interface is on a smartphone. When the access technology does not include the ability to photograph the check, another solution will be required.

5.1.1.4. Open Banking

Digital shekel end users will be able to benefit from open banking services – information services and payment initiation. Further analysis will be required in order to decide whether: The open banking APIs should be exposed by the PSPs (which may impose a significant technological burden on them),[62] or; By the backend or its associated databases (which may not align with the privacy policy of the digital shekel system, as these databases are not intended to hold detailed information on payment transaction history required for open banking information services), or; A combination of both.

Questions – Interoperability with Local Payment Systems:

41. This chapter describes use cases that integrate the digital shekel system with other means of payments, such as bank accounts (including batch payments), payment cards, and checks. How important is it for the system to support these use cases, and what complexities might arise from them? Please address some or all of the use cases in your response.
42. Are there alternative mechanisms for implementing these use cases that are preferable to those described in the document?
43. How important is it for digital shekel users to benefit from open banking services? For example, sharing financial information from the digital shekel wallet with other entities, or initiating a payment in the digital shekel wallet using another platform connected to the wallet based on open banking.
44. Does exposing open banking APIs impose a significant technological burden on system participants? Alternatively, can they be exposed by the backend layer without compromising user privacy?

[62] Currently, payment service providers that are not banks or credit card companies, and temporarily, also small new banks, are exempt from exposing APIs and do not participate in open banking.

5.1.2. With Payment Systems Abroad

"Cross-border payments" using the digital shekel will be possible in several ways.

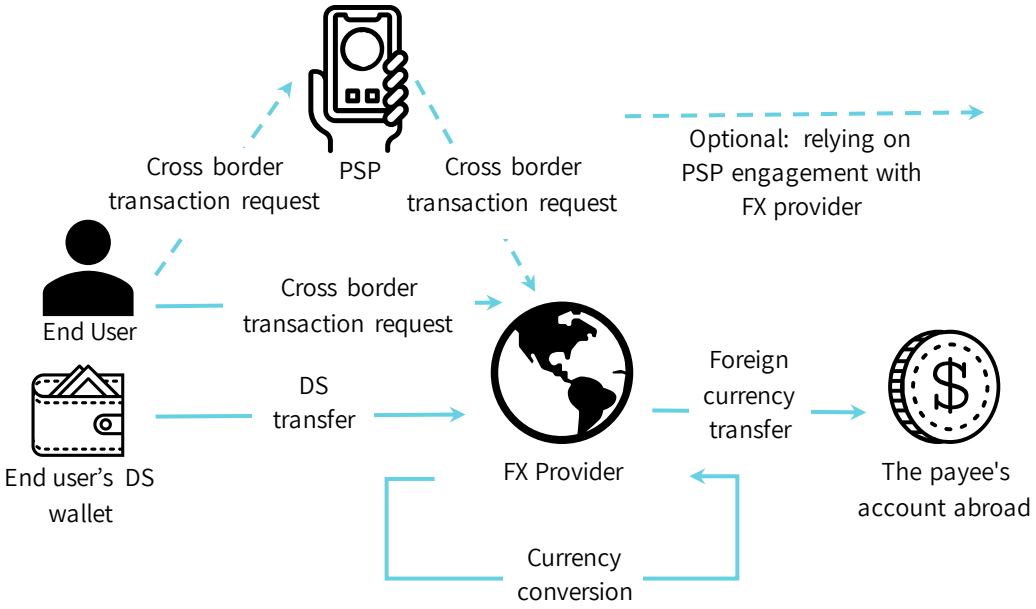
Digital shekel payments between an end user in Israel and an end user abroad, both operating within the digital shekel, are technically a straightforward. For example, Section 3.4.3 above specifies that businesses abroad can - under certain circumstances - hold a digital shekel wallet. Consequently, a payment between an end user in Israel and a business abroad will be executed as a regular digital shekel transaction.

5.1.2.1. Payments between the Digital Shekel and an Existing Payment System Abroad

Payments where one party uses the digital shekel and the other party uses an existing payment system abroad will rely on the existing connectivity between current payment systems in Israel and abroad. Various financial entities will act as "FX Providers", performing the conversion between the digital shekel and foreign currency, which may not necessarily be a CBDC:

- A transfer from a digital shekel wallet in Israel to a bank or eMoney account abroad will begin with transferring digital shekels from the end user's wallet to the digital shekel wallet of the entity acting as the FX Provider. From there, the process will continue as a regular cross-border transfer between that entity and the payee account abroad. The relationship between the end user and the FX Provider can be direct, similar to a customer approaching a money transfer service, transferring shekels to it, and having that service handle the transfer abroad. Alternatively, the end user's PSP may engage with such an FX Provider and offer the user the transfer service from the user's wallet to an account abroad based on this engagement.

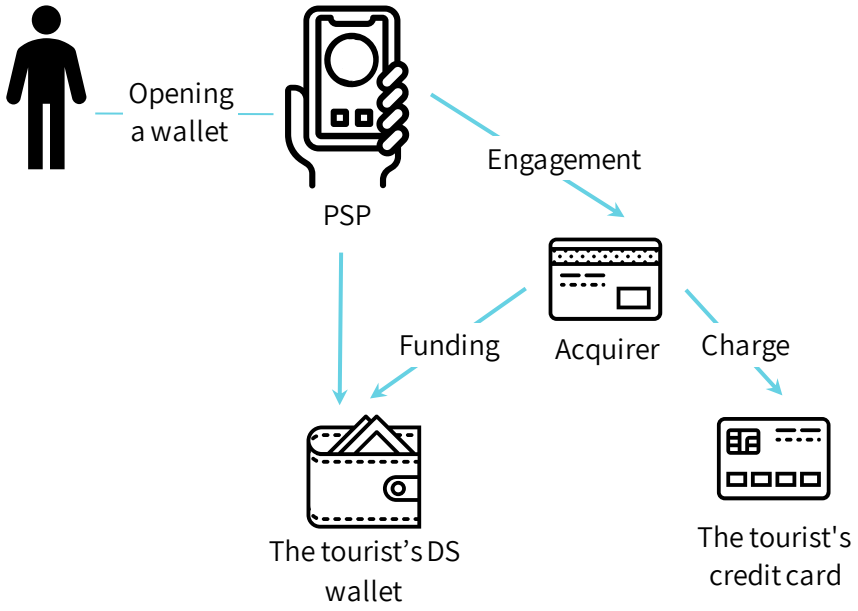
Figure 12: Transferring Funds from a Digital Shekel Wallet to a Payee Abroad



- In the case of an incoming payment to the digital shekel wallet, a transfer from an account abroad to a digital shekel wallet in Israel will be possible through an FX Provider, who will receive the payment from abroad and transfer shekels to the user's digital shekel wallet. The digital shekel wallet will also have a representation in the format of a bank account (see section 5.1.1.1), which will facilitate the transfer.
- Payments abroad using a debit card linked to a digital shekel wallet (see section 5.1.1.2). In this case, the card issuer will act as the FX Provider – receiving the charge from abroad through the international schemes, debiting the end user's digital shekel wallet, and transferring foreign currency abroad through the schemes, as is done today.
    - Tourists using the digital shekel will be able to fund their digital shekel wallets, opened for them by a PSP specialising in services for tourists, using their cards from abroad. The PSP will need to engage with an acquirer, who will transfer digital shekels to the tourist's wallet and charge the tourist's card through international schemes. One option is for the funding to be a one-time amount defined by the tourist, requiring the tourist to initiate funding again once the wallet is depleted. Another option is for each payment transaction in the tourist's wallet to initiate a "reverse waterfall" process, where digital shekels are transferred from the acquirer's

wallet to the tourist's wallet and from the tourist's wallet to the payee's wallet. At the end of the visit, the tourist will be able to defund the remaining digital shekels in the same manner.

Figure 13: Using the Digital Shekel by Tourists



These payment processes can be implemented based on the digital shekel's design, without relying on arrangements with foreign CBDC systems, to the extent that there will be any.

5.1.2.2. Payment From/To the Digital Shekel To/From a Foreign CBDC System

The most efficient way to conduct cross-border payments using the digital shekel should be through a platform that enables interoperability between different CBDC systems. Project Icebreaker (BIS et.al, 2023) demonstrated how such a platform can reduce risks and costs, increase competition, and enhance the potential for innovation in cross-border payments. Currently, no international arrangements for interoperability between rCBDC systems are

developing.[63] Nevertheless, it is possible to outline the necessary features of the digital shekel to ensure it can participate in such arrangements if they develop in the future:

- The messages in the digital shekel system should conform to an international standard. Currently, the most common standard is ISO 20022, but it is likely that adjustments to a dedicated CBDC standard will be needed. In this regard, it is worth noting FATF Recommendation 16, which sets "travel rules" for information about payment transactions.
- It should be possible to identify wallets in the digital shekel system according to an international identification standard, such as BIC and IBAN.
- When initiating a payment transaction in the digital shekel system, there should be an option to mark the transaction as one leg of a cross-border payment, so that relevant rules can be applied. Similarly, this should be possible when receiving a cross-border payment into the digital shekel system.
- The payment message should be able to include "proof of compliance" – a notification from the PSP that it has conducted the required checks regarding anti-money laundering, counter-terrorism financing, and other checks. Without such proof, the payment transaction will not proceed.[64]
- A PSP should be able to stop an incoming payment resulting from a foreign payment if it cannot verify that the foreign payment has passed the required checks and complied with the rules.
- There should be a mechanism to ensure that the digital shekel payment is returned to the end user if the international payment transaction is not completed for reasons beyond the control of the digital shekel system.
- The user should be able to see the exchange rate and the total fees that will be charged for the payment transaction before approving the transaction.
- It should be possible to receive confirmation from the international system that the foreign payment has been completed and present it to the digital shekel end user.

[63] Connecting the digital shekel to wCBDC systems could also streamline these processes.
[64] See: Bank for International Settlements. (2024). Project Mandala: Streamlining cross-border transaction compliance.

- The principles of immediacy and finality of the digital shekel will apply only to the segment of the transaction in the digital shekel (the transfer against the FX Provider on the shekel side), not to the side of other currencies.

Questions – Interoperability with Foreign Payment Systems:

45. What challenges arise from the mechanisms described for supporting cross-border payments in the digital shekel system? Are there preferable mechanisms to those described in section 5.1.2.1?
46. If international arrangements for interoperability between rCBDC systems do not evolve, are the features described in section 5.1.2.2 sufficient to ensure the system is prepared if of such arrangements evolve in the future?

5.1.3. With Digital Networks of Regulated Assets

With the development of the digital economy and the emergence of distributed ledger technologies (DLT), databases and networks are evolving where various assets are represented digitally, sometimes in the form of tokenisation. These assets range from financial assets to "real world assets" such as real estate, vehicle ownership certificates, and possibly even tickets to cultural events, plane tickets, etc., in the future.[65] Some trading in these assets occurs when the payment side of the transaction is based on the existence of "stablecoins" issued on the same network where the digital assets are issued. This allows for "atomic" transactions, where the exchange of the asset is conditional on the exchange of the money, and vice versa. Such transactions eliminate the "counterparty risk" present in a typical financial transaction.

The digital shekel will be based on a dedicated network.[66] However, the digital shekel system will maintain interoperability that allows for atomic or "near-atomic" transactions on networks of regulated digital assets against the digital shekel. One possible mechanism for

[65] Such use cases and their interoperability with the digital shekel were demonstrated in the "Digital Shekel Challenge."

[66] It may be decided otherwise in the future, for example, a "Unified Ledger" as described in: Bank for International Settlements. (2023). Annual report 2023.

such interoperability is an API that supports a HTLC smart contract,[67] which allows for the execution of a transaction in the digital shekel to be conditional on a parallel transaction in an asset traded on another digital network, without relying on a third-party intermediary.[68] Another option is to use a trusted ASP as an orchestrator.

Questions – Interoperability with Digital Assets:

47. How important is the connectivity of the digital shekel system to regulated digital asset systems? For example, a connectivity that will enable executing a conditional payment in the digital shekel against the transfer of a virtual asset in a DeFi transaction?
48. What challenges might arise from such connectivity? Are there additional mechanisms to enable it, besides those described in the section, such as alternatives to the HTLC mechanism?

5.1.4. With National Databases and Information Systems

A payment system needs to be continuously updated with information from public and national authority databases. The ability to extract relevant information immediately, continuously, and automatically streamlines the operation of the payment system, allowing it and its participants to hold a minimum amount of information, avoid holding unnecessary information, efficiently verify existing information, and prevent errors resulting from manual data entry. For this purpose, the system needs to be able to read or receive information from other digital systems.

The digital shekel system will strive for interoperability with public and national information systems, according to the capabilities of these systems to support it, in accordance with the law and regulatory rules, and without compromising the privacy policy of the digital shekel system (see chapter 7.1). The system will be able to interface with these systems according

[67] Hash Time Lock Contract. This mechanism was tested both in Project Icebreaker and in one of the use cases examined in the "Digital Shekel Challenge."
[68] See more in chapter 5.2.1 "Conditional and Advanced Payments."

to their mechanisms of sharing information[69]: At the user level (e.g., information from the Population Authority or the Companies Registry used by PSPs for "know your customer" actions), or at the level of the central systems operating alongside the backend system (e.g., the alias management system, described in section 3.2.1).

Questions – Interoperability with National Databases and Information Systems:

49. Which national systems should interface with the digital shekel system?
50. How can connectivity between the digital shekel system and national information systems be enabled without compromising the privacy principles of the digital shekel?

5.2. Innovative Payment Use Cases

The Digital Shekel system will offer functionality and define conditions and rules that support the development of advanced and complex use cases, reducing dependence on specific participants and the likelihood of "walled gardens" that could harm competition and network effects.

There are various possibilities regarding the extent to which the core of the digital shekel system would be involved in how users perform different activities in the system. For example, the system can offer a basic level of functionality, allowing only simple processes such as onboarding the system, receiving a wallet, funding it, and performing basic payment transactions. This approach places full responsibility on private sector participants to develop capabilities that help users carry out more complex activities. Under this approach, users can benefit from advanced functionality offered by participants, but their dependence on specific participants will increase, the risk of 'walled gardens' will grow, competition may

[69] For example, the Population Authority's API allows for verifying a person's identity and registration in the authority's databases (see an example of a request form for banks) (Link only available in Hebrew).

be harmed, the network effect will be reduced, and all these could also limit the innovation offered by the digital shekel system as a whole.

Therefore, the digital shekel system will also offer advanced functionality at its core as a basis for supporting participants' ability to offer complex and advanced use cases, as detailed further below. This will allow the digital shekel system to enable various participants to operate within a 'level playing field.' Consequently, users will be able to enjoy advanced use cases even if they are not offered by the PSP managing their wallet (for example, by linking the wallet to an ASP), and without any dependence on the identity of the PSP of the end user with whom the transaction is conducted.

5.2.1. Conditional Payments

A conditional payment is the ability to initiate a payment when predefined conditions are met. The process for executing it includes the following steps:

1. The business logic for performing the payment transaction is defined;
2. Funds are locked in the payer's wallet (if necessary, depending on the business logic);
3. The realization of the conditions for the payment transaction is monitored;
4. If the conditions are met, the payment is executed.

The business logic defined in step 1 above can be classified into three types (table 3):

5.2.1.1. Time-Based Business Logic

Initiates a payment transaction when the time condition is met. Given that some time-sensitive payment transactions require very high precision — down to the second or even more precise—and considering potential time discrepancies between participants' systems, the system will provide a unified date and time as well as a timestamp on the payment transaction. Participants can define payment transactions based on the system time, ensuring they are triggered when the specified time condition is met.

Table 3: The Business Logic of Conditional Payments

Business Logic Based on		Examples of Use Cases
Time		Standing Order for Monthly Transfer
Usage	User Characteristics	Payment Restriction to Specific Industries
	Usage Characteristics	
	Pay as You Go	Electric Vehicle Charging
External Condition		Verification of Delivery Receipt Confirmation of Authorised Signatories' Consent for the Transaction Verification of Asset Transfer on Another Digital Network

5.2.1.2. User and Usage-Based Business Logic

Usage-based payments pertain to both a simple user experience as part of a basic digital shekel journey and to an advanced user experience, allowing the wallet owner to condition payments based on user characteristics, specific usage characteristics, and consumption volume of the product or service. For example, a business can define the types of uses an employee can make when accessing the business wallet. To facilitate this, the system will establish uniform standards for sharing information between participants during payment transactions, including details about the types of users involved in the transaction, industry sectors, and other relevant factors.

5.2.1.3. External Condition-Based Business Logic

An external condition is any event that occurs outside the system, such as the delivery of a product, the transfer of another digital asset on a different network, the result of a sports game, a stock price reaching a certain target, etc. While the verification of the external condition will be performed by participants (possibly in combination with external services), the system will support the ability to lock funds in the end user's wallet for the future execution of the transaction. This includes defining the lock duration and conditions for its release, receiving information about existing locks in the wallet, and executing or canceling the lock in various configurations of participant involvement, according to the following mechanisms:

1. **Two-Party Lock**: This involves locking an amount in digital shekels in the payer's wallet where the trigger for executing or cancelling the lock is sent by the PSP of the payee. This type of lock was implemented in the "Digital Shekel Challenge" in use cases such as the purchase of air tickets by an AI agent, which withdraws the locked funds only if the travel service provider delivers the service. Another example was a platform assisting people in debt, which allows fundraising to support them. The raised support amount is locked for the debtor and released upon meeting the set targets.
2. **Three-Party Lock**: This functionality enables the involvement of a third party (not the PSP of the payer or the payee) where the trigger for executing or cancelling the lock is sent by the third party. For example, an ASP providing services to the payee may initiate the lock with the payer's PSP. This type of lock was implemented in the "Digital Shekel Challenge" in use cases where an ASP confirmed that work that was ordered was completed and then released the funds that were locked against the work. It was also used in scenarios where an ASP verified that a digital asset was transferred from the seller's wallet to the buyer's wallet on a blockchain, then released the locked digital shekels as payment for the digital asset.
3. **Hash Time Lock Contract (HTLC)**: This involves locking digital shekels based on the HTLC mechanism, where the trigger for executing the lock is based on the use of a "Secret" or any other mechanism commonly used in digital asset networks that allows the same business logic. For example, the transfer of a digital asset on an

external network can be conditioned on the transfer of digital shekels in return, using HTLC, where the 'Secret' used to execute the asset transfer on the external network also serves to transfer the locked funds on the digital shekel network as payment for the digital asset. This type of lock was implemented in the "Digital Shekel Challenge" in use cases demonstrating payment for a digital asset transferred from a seller to a buyer, where the release of the locked funds from the buyer to the seller is based on a mechanism built by a third party, but without the third party's involvement in releasing the locked funds.

5.2.2. Additional Advanced Capabilities

Alongside conditional payment transactions, and as part of supporting an 'advanced' user journey, the digital shekel system will also offer advanced functionalities to support various use cases, some of which have already been mentioned in this document: waterfall mechanism, sub-wallet management, split payments, and batch payments. Another functionality not yet discussed is wallet status management: freezing the wallet, allowing it to continue receiving funds but not making payments (e.g., as a safety measure in case of loss of access technology), and disabling the wallet (stopping all activity in the wallet, but as a reversible action, without completely disconnecting the wallet from the digital shekel system).[70]

Many of these processes do not require the support of the digital shekel system's core, as participants can offer them based on the functionality the system provides to support a 'basic' user journey. However, for others, the core system must be involved in the process. Table 4 presents advanced capabilities in the digital shekel and explains how they can be performed, with or without the involvement of the core system:

[70] These capabilities were also demonstrated in the "Digital Shekel Challenge."

Table 4: Involvement of the Core System to Support Various Advanced Functionalities

Topic	Functionality	Necessary Involvement of Core System?	Explanation
Secondary Wallet	Linking a secondary wallet to the primary wallet	No	Based on the proposed design of the backend layer, an end user can open multiple wallets at the central database, with the PSP managing the hierarchy between the wallets.
Wallet Status Management	Ability to freeze or temporarily disable a wallet	Yes	Given the approach where multiple PSPs can operate on a single wallet in the system, the wallet status needs to be managed centrally.
Split Payment	Split payment – a single payment transaction to multiple beneficiaries in one transaction	Yes (partially)	At a minimum, the system will need to support the PSPs ability to verify whether the payee are existing and valid, as if one payment cannot be completed the whole transaction needs to be aborted.
	Batch payment – a series of payments from a single entity to multiple independent beneficiaries	No	A sequence of payment transactions that the PSP can transmit independently of the system's support.
Messages between Participants	Request to lock / Request to Pay	No	Participants can use existing infrastructures for bilateral communication, such as the open banking infrastructure.
Funding and Defunding	Waterfall Mechanism	No	PSPs will be able to support this functionality based on the logic defined with the user/system rules and the option to perform redemption, which will be available at core system.
	Reverse Waterfall Mechanism	No	Payment providers will be able to perform a funding (supported by the core system) automatically ahead of a payment transaction.

Below is a summary of the advanced capabilities that the core of the digital shekel system will support, considering the overall requirements to facilitate an 'advanced' user journey and enhance efficiency and innovation within the system:

- Information regarding system time and transaction execution time;
- Support for micropayments;
- Locking funds in the end user's wallet;
- Defining the lock duration;
- Information on existing locks;
- Drawdown or cancellation of a lock in various configurations of participant involvement in the process (Two/Three party) and the method of lock (e.g., HTLC);
- Support for split payments (Split and Batch);
- Support for wallet status management, including the ability to freeze and temporarily disable a wallet;
- Offline payments.

It is important to emphasise that the ability to perform conditional payments and utilise various advanced capabilities does not pertain to the money itself. **The digital shekel will not be programmable money and will not contain rules regarding its usage possibilities.** This condition is necessary, among other things, to ensure that the digital shekel will always be at par (1:1) with cash.

5.2.3. Adding New Functionality for All System Users

In general, the advanced functionalities will be accessible to all participants through the system manager, who will have the authority to implement changes, cancel them, and add additional functions to support advanced use cases. Decisions regarding additions to the core system's capabilities will be based on ecosystem needs, efficiency considerations, and maintaining a clear distinction between functionality supported by the central bank and that fully developed by system participants. Additionally, when defining advanced functionality in the core system, the needs of participants and users for whom the Bank of Israel will act as a PSP will also be considered. This includes features such as an automatic mechanism for

collecting merchant fees by the PSP, an automatic mechanism for managing FI liquidity, a trigger for payment at predetermined times by a government office, etc.

Questions – Innovative Payment Applications:

51. This section describes innovative payment applications that the digital shekel will support. Are there additional applications that the digital shekel can enable that were not mentioned? Are any of the mentioned applications unnecessary?
52. What complexities might be associated with the advanced functionalities described in this section?
53. Is it appropriate that only the central bank will be able to add functionalities to the system? Should this capability also be extended to system participants or other entities (e.g., through decentralised technology or open source)?

5.3. Offline Payments

The Digital Shekel will enable offline payment transactions – transactions performed without communication between the users' access technologies and the PSP, and without communication with the backend layer. An offline wallet will need to interface with the PSP after exceeding a threshold of transactions actions for system updates and wallet data synchronisation with the PSP (except for transactions defined as anonymous).

Final payments in the digital shekel can also be made offline, a capability traditionally associated with physical cash.[71] While this feature may seem basic from a user experience perspective, it is included in the advanced user journey chapter due to the technological complexity involved. This capability is important for several reasons:

- **Payments in areas without communication**: For example, areas without cellular coverage or with temporary or localised communication issues, including temporary damage to systems due to security incidents, technical failures, or natural disasters.

[71] Payment cards can be used for transactions without a network connection, but the clearing is not final and is exposed to credit risk.

Expanding accessibility to these areas increases the usability and certainty of using the digital shekel for the entire potential user population, enhancing its attractiveness.

- **Redundancy**: In the event of an online system failure, the ability to make offline digital payments is a crucial component in creating a resilient and stable payment system. This reduces dependence on internet and cellular infrastructure and increases the overall resilience of the payment system in an era of declining cash usage.
- **System performance improvement**: Supporting continuous payments, even when connectivity issues or disruptions in the central system may arise, will enhance the continuity and reliability of the digital shekel system as a whole. Offline payments can help reduce the load on the central settlement engine and various system components (the weak links, especially during peak hours) and allow for emergency maintenance or upgrades to the central system without a complete shutdown of payment services.

On the one hand, the use and holding of offline digital shekels reduce certain risks to the system by enabling payment capabilities anywhere, regardless of communication with the central system, including in emergencies. On the other hand, this capability introduces additional risks:

- **Monitoring and enforcement challenges**: Offline transactions cannot be monitored in real-time, limiting the ability to detect suspicious activities such as money laundering or financing of terrorism. Additionally, enforcing holding limits or other system policy restrictions is challenging.
- **Data loss and financial risk**: In the event of loss or theft of the access technonlogy (e.g., a device with an offline digital wallet), there is a significant risk of losing funds. Transaction information since the last synchronisation with the PSP system cannot be recovered.
- **Vulnerability to physical attacks and counterfeiting**: Offline transactions are not verified through central system clearing, increasing the risk of theft, robbery, or attempts to counterfeit and double spend.

- **Data inconsistency**: Offline transactions may create inconsistencies between data in different wallet regarding the same transaction due to the lack of real-time supervision.

Some of these risks are further exacerbated if offline transactions are also anonymous, as the difficulty in monitoring and enforcement significantly increases. The design of the offline digital shekel aims to address these risks while maintaining the best possible user experience. Here are the main design points:

In the backend Layer, a central wallet will be defined to represent the holdings of all users in offline digital shekel wallets. When a user requests to convert online digital shekels to offline digital shekels, the user's offline wallet must be connected to the network. The digital shekel system's settlement engine will debit the user's online wallet and credit the central wallet. Simultaneously, the "offline DS issuance engine" will issue offline digital shekels to the user's offline wallet. In the opposite direction, when converting offline digital shekels back to online digital shekels, the user's wallet will transfer the offline digital shekels to the "offline digital shekel issuance engine," which will delete them, and the settlement engine will debit the central wallet and credit the user's online wallet.

The offline digital shekel balance will be stored in the secure container of the access technology. For non-anonymous transactions, the required transaction details will also be stored, similar to online transactions. These details will be synchronised with the PSP systems during interfacing (see below). An offline wallet must be on a single access technology. For caution and transparency, the PSP will be required to inform the user (in a manner determined by system rules) that losing access to the offline wallet means a potential loss of the stored value. No interest will be paid on offline digital shekels, even if interest is paid on online digital shekels.

Every PSP will be required to provide its customers (if requested) with an offline digital shekel service and wallet. If hardware is involved, the PSP may charge a fee. Payment activities defined as a basic service without cost to the user in online digital shekels will also be free of charge when provided offline. Funding offline digital shekels will be from the same user's online wallet, and payment transactions between different users' online and offline wallets will not be allowed. ATMs will enable funding offline digital shekels against cash. For this

purpose, ATMs will hold an offline digital shekel wallet[72] and allow cash withdrawals against offline digital shekels and cash deposits to the offline digital shekel wallet. ATMs will also enable software and wallet restrictions updates, among other things, for business continuity in case of network failure (assuming the ATM still has communication). Such funding will also be possible at some FI counters.

Every offline wallet will be required to synchronize periodically with the PSP systems. An offline wallet that is not synchronised according to the rules will be frozen (cannot make payments; can receive funds, as long as it does not exceed the holding limit). The synchronization requirement will be determined by the volume of outgoing payments:[73] The secure container will count the amounts of outgoing payments from the wallet. After reaching the limit, all outgoing payment transactions will be frozen until the wallet is synchronised. During synchronization, all transaction data (that is non-anonymous) will be uploaded to the PSP systems and deleted from the secure container (data may be saved on the user's end device). If necessary, the PSP will update the wallet with changes regarding restrictions and limits according to the system manager's instructions, with PSP rules or customer requests, software updates, lists of suspicious wallets (in the context of fraud or AML), and various other parameters. Merchant fees and other charges related to offline payment transactions will be locked in the secure container of the payer, and withdrawn for the beneficiary (in the case of merchant fees, the PSP, for example) automatically during the synchronization.

To address various risks, the system can implement restrictions on offline activity (transactions and holding). These restrictions can vary by user types and even at the individual user level. PSPs will have the option to set a transaction amount limit (per transaction/period) and a holding amount limit in wallets. The PSP will configure the offline wallet to prevent receiving amounts that exceed the defined limit, and a wallet in this state will not be able to receive funds. When opening any offline wallet, the user will be required to allocate part of their general holding limit[74] for the offline wallet. For this purpose, the

[72] Criteria will be set to decide which ATM operators must provide this functionality and which do not.
[73] If a secure solution for using a time counter from the last synchronization will be available in the future, this mechanism will be preferred.
[74] See section 7.6.

secure container will allow managing variable holding limits, dictated during interfacing with the PSP systems. For managing the holding limit, this allocation will be deducted from the user's online holding limit, whether the offline holding limit is utilised or not. The PSP can set stricter limits for their customers than the system limit, for risk management reasons. An offline wallet will be limited to the lower of the system requirements, user request, or PSP decision. In any case, the limit will not be less than a minimum set by the system to prevent misuse of the PSP's ability to impose such limits.[75]

If an offline transaction is also defined as anonymous, identifying details on it will not be synchronised or will be synchronised anonymously. To mitigate the inherent risk in such transactions, the amount of a single anonymous transfer and/or the amount for a period will be limited, according to the restrictions applied to anonymous payment transactions in general.

Some offline wallets will have "active communication" capabilities – independent communication, including a power source (e.g., a smartphone app). Other wallets will have "passive communication" capabilities. These will be wallets without independent communication or power source capabilities (e.g., a payment card with a smart chip) and will need to rely on an active communication end device or a bridging device. When a wallet with passive communication capability performs a payment transaction with an online end device, synchronizing with its PSP will be done through the PSP of the online device. The data will be transferred in an encrypted manner that can only be decrypted by the PSP of the passive wallet.

Questions – Offline Payments:

54. The Offline use of the digital shekel can enhance the user experience and support the redundancy of the payment system in Israel. However, it introduces potential risks not present in online payments, such as loss of money in case of device loss, fraud risks, and others. That Given, how important is it to enable offline use of the digital shekel?
55. How can the risks involving offline payments be mitigated? Are there additional risks related to offline use of the digital shekel that were not described in the document?

[75] For example, to prevent PSPs from not offering an offline wallet service to certain customers.

56. Is it appropriate to require every PSP to enable offline use of the digital shekel for their customers?

6. Architecture and Technical Issues

6.1. The Backend Layer

At the core of the digital shekel system lie the main database and the settlement engine. Neither the settlement engine nor the main database will store any personal identifiable information about end users or details of individual transactions conducted in digital shekels, at any stage.

In addition to the main database, additional databases will collect operational and statistical information in a manner that upholds privacy principles.

At the core of the digital shekel system lies the settlement engine, alongside to it the main database which records balances in the end users' digital shekel wallets. The settlement engine itself does not store information;[76] rather, it updates balances in the database, thereby completing payment transactions between wallets and ensuring their finality.

The only entity authorised to make any changes to the records in the main database (updating balances following settlement or issuance, adding a wallet following a user onboarding the system, etc.) is the system operator. System participants, depending on their role and the permissions granted by the system operator or by end users, can read the information in the database or request the system operator to modify it (e.g., perform a payment transaction).

The main database will include only the minimal information required to fulfil the two roles of the system manager:

1. Settling payment transactions: For the system operator be able to fulfil its primary role – settling payment transactions - the main database will include, for each end user, at a minimum: the unique identifier issued to them upon onboarding the

[76] Operates in stateless mode.

system (see section 4.1), the list of wallets associated with this unique identifier, the balance in each online wallet, and the identity of the participants (PSP,ASP) linked to the wallet.

2. Enforcing Policies and generating operational and statistical data: The main database will need to include static information about each wallet, such as the sector to which the wallet belongs (private sector distinguishing between adult/minor/Israeli/foreigner, business sector distinguishing by business size, government, financial, etc.). This information is required for enforcing policy rules, such as holding limits (which vary by sector) or interest payments (which may also vary by sector and the balance in the wallet at any given time). Additionally, this information will be used to generate aggregate statistical data (e.g., information about the total balance held by individuals).

In any case, it will not be possible to link the information in the main database with information about transactions conducted in the system, and certainly not with the identity of end users or any other personally identifiable information ("PII").

Although the main database will contain information about the identity of the PSP to which the wallet is linked, this will have no impact on the settlement of transactions. Specifically, transactions between two wallets associated with the same PSP will be handled in exactly the same manner and at the same speed as transactions between two wallets associated with different PSPs.

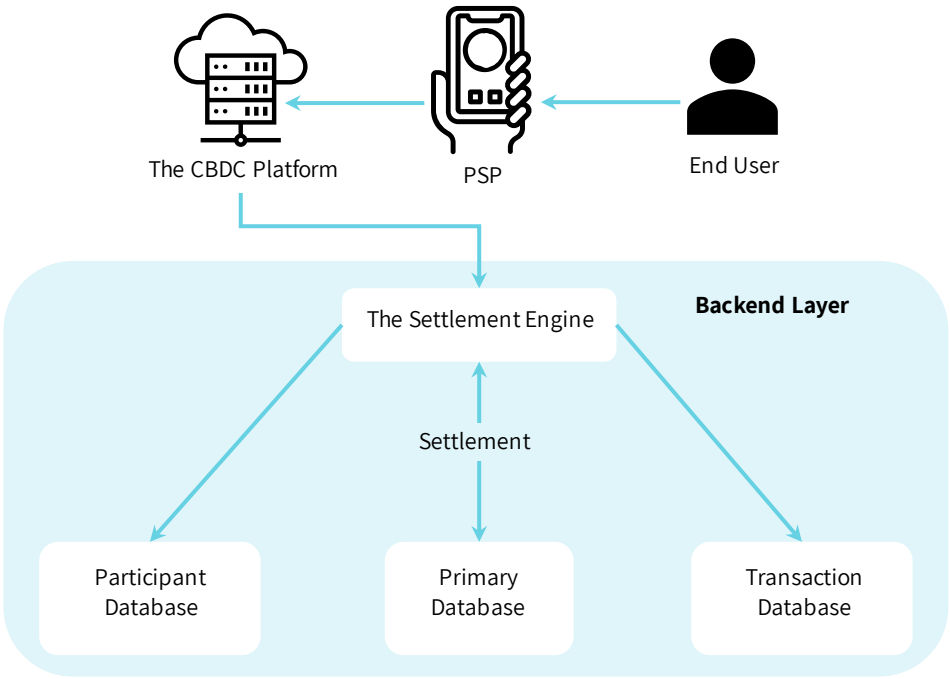
Alongside the main database, there may be additional databases where information required by the system manager for purposes other than settling transactions will be stored. This includes information needed to ensure the proper functioning of the system, analyse the adoption and use of the digital shekel as a means of payment, support conflict resolution between participants, analyse policy measures and their impact on system activity (applying interest, changing holding limits, etc.), perform statistical analyses, and more. Another database that will certainly exist is an aggregate database of payment transactions, which will allow for comprehensive analysis of system activity characteristics. For example, when the settlement engine updates the balance in two wallets in the main database following a payment of 50 Shekels from a private user to an online merchant, the transactions database

will be updated, recording a remote transaction (as opposed to a physical transaction at the POS) in the size group of 0 to 500 Shekels in the P2B activity sector. Here too, it is important to emphasise that the information in the additional databases cannot be linked to the identity of users or any other personally identifiable information.

Another database will include information about system participants. This information will be broader than the information about users, as participants are not entitled to the same level of privacy against the system manager. The static information about participants will include, in addition to the unique identifier, the name and type of participant, and in the case of a PSP that chose to specialise in a certain user sector[77], the sector it serves, etc. The system manager will be able to identify which wallets in the system belong to each participant. However, there will be a distinction between wallets used for the participant's activities (e.g., a wallet used by a PSP to collect fees, or a wallet used by an FI to fund user wallets) – for which the system manager will have full information – and wallets used by the participant for end-user activities (e.g., for salary payments or supplier payments), for which the same privacy policy as for other business user wallets will apply. The broader information about participants in the main database will allow for the creation of broader information in the transactions database. For example, if a business pays a 5 Shekel fee to a PSP, a transaction in the size group of 0-500 Shekels in the "fee payments" activity sector from an un-identified business to an identified PSP will be recorded. If a PSP pays an interchange fee to another PSP, the transaction will be recorded with the identifying details of both PSPs. However, if a PSP pays a salary to its employee, the transaction will be recorded without the identifying details of the PSP or the employee.

[77] As described in section 3.3.1.

Figure 14: A Close Look at the Backend Layer



Additional components of the backend layer include the central offline digital shekel wallet, to which the transfer (and removal from circulation) of digital shekels from an end user's wallet when the user wishes to convert online to offline digital shekels (and vice versa, as described in section 5.3). Another key component is the mechanism for issuing digital shekels against cash, as detailed in section 4.3.2.

It should be emphasised that the description of the backend layer in this section is a logical framework and does not prescribe any specific technology for implementing the described logic. In particular, this logic can be realised using distributed ledger technology (DLT) or conventional technology.

Questions – Backend Layer:

57. Does the proposed logical architecture support the necessary functionality to facilitate the user journey while upholding the privacy principles of the digital shekel?
58. Does the logical description of the backend layer adequately serve the required functionalities of the digital shekel, such as enforcing holding limits, enabling tiered interest payments, allowing end users to hold multiple wallets with multiple PSPs, etc.? Are there additional components and services that should be included in the backend layer?

6.2. Digital Shekel Transaction Message and Communication between Participants

An online payment transaction between two end users necessitates the transmission of a payment message between the PSPs and the settlement engine. This payment message will include at least the minimal information required to execute the transaction, without exposing identifiable information to the settlement engine. The structure of the payment message will be designed flexibly to allow for the inclusion of additional information as needed.

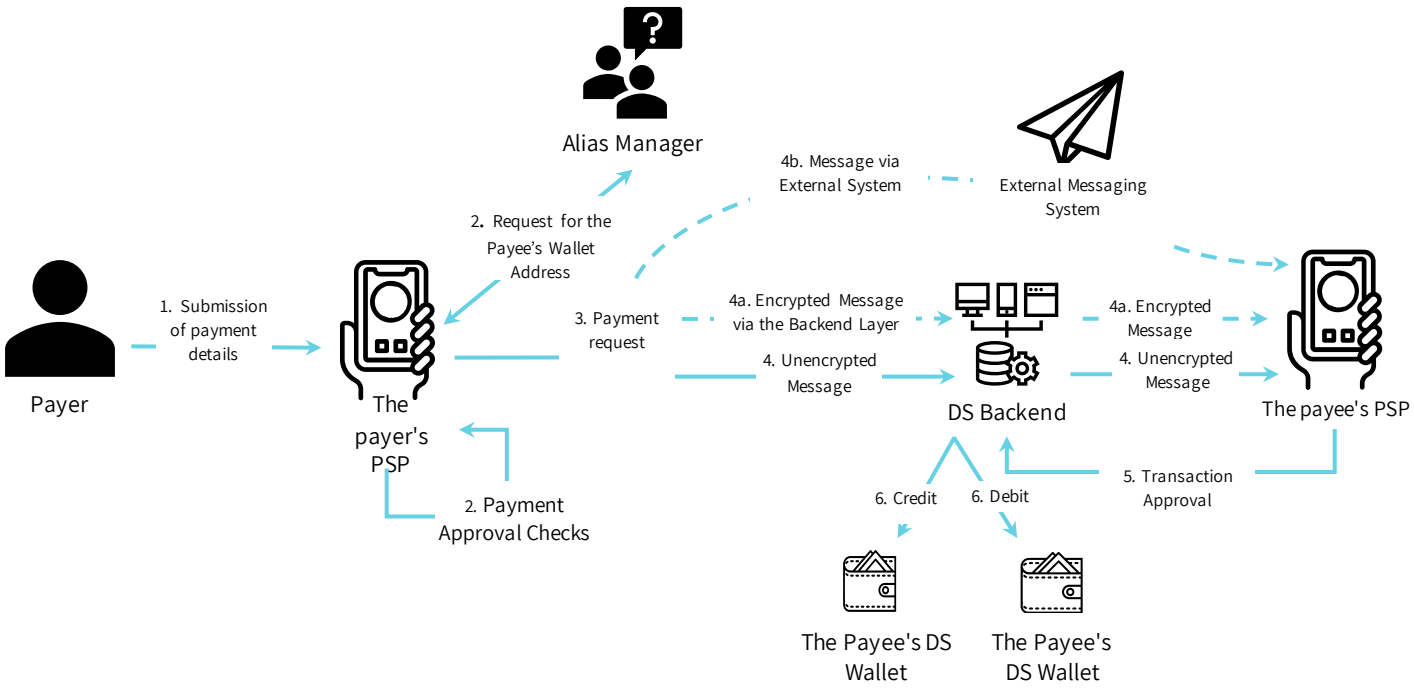
Every process within the digital shekel system, particularly a payment transaction, requires communication between the various entities in the ecosystem. Let us analyse a simple payment transaction as an example (Figure 15):

1. The end user wishes to perform a payment transaction. They contact their PSP through the user interface, providing the payment amount, the alias of the payee, and any additional details as desired or required (e.g., the reason for the payment).
2. The payer's PSP contacts the main database to verify that the user has sufficient balance to perform the payment.
3. The payer's PSP contacts the alias management system to obtain the payee's wallet address.

4. The PSP conducts the necessary checks (e.g., anti-money laundering) and approves the payment.
5. The payer's PSP sends a request to the settlement engine to perform the payment transaction (payment message) from the customer's wallet to the payee's wallet. The message includes information that is partially visible to the backend layer (transaction amount, payer and payee wallet addresses, additional wallet attributes for aggregate information to be stored in additional databases) and partially not visible to it (e.g., the identities of the payer and payee). Information that should not be visible to the central bank can pass through the backend layer in encrypted form or through an external communication system (e.g., the open banking system).
6. The payment message in all its parts reaches the payee's PSP, which conducts the necessary checks to approve the receipt of the payment (anti-money laundering, the wallet's ability to receive the payment without exceeding the holding limit, etc.).
7. The payee's PSP approves the settlement engine to perform the payment transaction.

To enable each of the steps in performing the payment transaction described above, it is necessary to define the structure of the payment message, the mandatory information items that must be included, optional information items, the method of transmission between participants, and the information each entity in the chain will be exposed to. To facilitate connectivity between the digital shekel system and other payment systems, both domestically and internationally, the payment message should comply with an accepted international standard. At the time of writing this document, the accepted standard is ISO 20022. However, as described in section 5.1.2, it is likely that an adapted standard for CBDC will be required, either as an evolution of ISO 20022 or from another standard.

Figure 15: Message Transfer in a Payment Transaction



The payment message will include, at a minimum, the basic identifying details about the wallets or end users involved in the payment transaction and the participants involved in it. The message structure will allow for the inclusion of additional details such as broader identifying information about the users and participants, and additional information that may be required for different types of transactions (e.g., the payee's ID number in the case of salary payments, the participant's wallet details for cross-fee payments, etc.), as described in table 5. The message will be characterised by maximum flexibility to include additional information as required for the transaction – for example, information that can be shared in encrypted form with the central fraud prevention system (see section 3.2.2), without being exposed to other entities in the digital shekel system. Additional information items can be added to the message that could be used in the future for additional databases, for services that the Bank of Israel or the private sector may offer in the future.

Table 5 – Information Items in the Message for Processing a Push Payment in the Digital Shekel System

Object	Examples of Information Items	
Link to Message Title	Message Identifier	
	Date and Time of Request Submission	
Payment Transaction Characteristics	Payment Type (Salary, Payment, Other)	
	Amount to Transfer	
	Transaction Type (Remote or Physical)	
	Additional Text (e.g., Reason for Transfer)	
Payer	**Minimal Information Items**	**Extensions According to Usage Scenario**
	Wallet Details in the System	Name
	Alias (This information is not necessarily shared with the creditor)	Identification Number
Participant Handling the Payer	PSP Identifier in the digital shekel System (PIC)	
Participant Handling the Payed	PSP Identifier in the digital shekel System (PIC)	
Payee	**Minimal Information Items**	**Extensions According to Usage Scenario**
	Specific Identifier or Wallet in the digital shekel System	Name
	Alias	Identification Number

The payment message can be transmitted between participants through the backend layer, in which case parts of it will need to be encrypted to ensure, in accordance with the system's privacy principles, that they can only be read by the participants and remain invisible to the backend layer. Alternatively, the message can be transmitted through an external communication infrastructure (e.g., the open banking infrastructure). Once the participants have settled all the necessary conditions for the transaction, they will then transmit the required information to the backend layer to execute the transaction.

Questions – Payment Message:

59. What principles should guide the construction of the payment message to support business needs while maintaining the principle of privacy by design?
60. Is it appropriate to base the payment message on the ISO 20022 standard? What other standards for payment messages might be relevant, and what are their advantages and disadvantages?
61. Should the payment message be transmitted between participants through the backend layer or via an external communication infrastructure (e.g., the open banking infrastructure)? Where should such infrastructure be managed?

6.3. System Performance

The Digital Shekel system will be available to end users 24 hours a day, every day of the year (24/7/365), with availability as close to 100% as possible. The time to completion and finality of a payment transaction will be no more than a few seconds.

Performance requirements will be consistent for all participants, ensuring that the end user enjoys optimal performance in their digital shekel experience regardless of the participant serving them.

The settlement engine can process scheduled payments during periods of lower activity load.

The system will be designed with an emphasis on scalability to accommodate growth in usage volumes.

To ensure a high level of performance and redundancy, the digital shekel system will be designed to operate - at least for basic payment transactions – independently of other payment systems, except for funding and defunding digital shekel wallets.[78] To maintain

[78] Funding and defunding, as well as waterfall and reverse waterfall, depend on the availability of the FIs' current account systems, and cash funding and defunding depend on the ATM switch, as described in section 4.3. The digital shekel system depends on the availability of the RTGS system for issuance and redemption of DS, but these actions are performed periodically and are not expected to be affected by temporary unavailability of the RTGS system. Dependence on other systems such as the MASAV faster payment system or credit card schemes will exist for payment applications requiring interoperability, as described in section 5.1.

high availability, the system manager will establish processes to handle situations of unavailability within the system itself or in supporting systems (such as electricity, internet, etc.), if necessary, in collaboration with other state authorities. Under normal conditions, the unavailability of core systems (such as the settlement engine, PSP systems and communication between them) should be rare and of very short duration, with defined recovery processes and predefined recovery time objectives (RTO) and recovery point objectives (RPO).

As part of the KPIs defined by the system manager, the time to completion and finality of a regular digital shekel payment transaction (latency) will be no more than a few seconds (after all required checks to complete the transaction, such as anti-money laundering checks, have been performed). However, the system will also support "scheduled payments," where the time between initiation and completion and finality can be longer (e.g., up to about two hours). This capability is mainly suitable for asynchronous payment where the exact time of receipt is not critical, allowing some payment transactions to be shifted to periods of lower system load (e.g., salary payments initiated by employers at night and completed by early morning, etc.).

The system manager will define KPIs for the system operator and participants. These KPIs will be established to ensure that the end user's experience is not adversely affected by loads on core systems. To achieve this, participants and their system providers must also adhere to appropriate KPIs, taking into account the expected loads on their systems, communication systems, and the backend system. KPIs will be the same for all participants of a certain type, ensuring that the end user enjoys optimal performance in their digital shekel experience regardless of the PSP through which they are connected to the system or the FI from which they fund their wallet.

In full adoption, the digital shekel system may need to support a very high number of transactions per second (throughput), which cannot be estimated at this stage and may not be estimable during system setup. Therefore, it is important that the system is designed and built to be scalable, with scalability achievable quickly and at a marginal cost that decreases as the volume of transactions in the system increases. For this purpose, system components that need to scale horizontally will be separated from those that need to scale vertically. The

Bank of Israel will examine the system's ability to support various adoption scenarios (e.g., low, medium, and high adoption scenarios) and the ability to scale the system from one scenario to another. All system participants will be required to consider these scenarios when setting up their systems and test them accordingly. The system manager will continuously collect and analyse information about system performance, and participants will collect and report to the system manager the information that allows monitoring their compliance with performance requirements and various KPIs.[79]

In designing the system, the need to avoid making the backend layer a bottleneck will be considered. For example, computational processes that do not need to be performed in the core system, such as cryptographic validation, will be performed away from the core. The functionality that the backend layer makes accessible to participants (e.g., API calls) will be designed so that the calls are independent of each other, allowing a call to the system to be made without dependence on another call.[80]

Questions – System Performance:

62. Considering the design requirements and the importance of high system performance, which key functional requirements described in the document might burden the system's performance and related systems, and how can they be addressed?
63. What mechanisms can be considered to handle loads and improve system performance? For example, can the described "scheduled payments" mechanism effectively manage the load created by payments such as salary payments?
64. Should the system's performance targets (availability, latency, throughput) be similar to those of existing payment systems or are more ambitious targets required from a future perspective?

[79] The relevant information will have different layers. For example, information about the response time from the moment the end user entered a payment transaction request until it reached the PSP systems, the time from when the request was received until it was sent to the settlement engine, etc.
[80] Even if at the application level there are processes that require a sequence of calls, at the infrastructure level, the ability to perform each call separately may help manage loads by processing the calls using parallel servers.

7. Policy, Rules, and Regulation

7.1. Privacy

The Digital Shekel system will be designed with a focus on maintaining user privacy (Privacy by Design).

Neither the Bank of Israel nor any other central entity will have the ability to access personal identifiable information about the activities of end users in the digital shekel system.

The level of privacy in the digital shekel will be higher than that of existing digital means of payments but lower than that of cash.

Participants will not be able to use the information they accumulate about users and their activities in the digital shekel system for commercial purposes unless users give clear and informed consent.

The digital shekel will allow for anonymous payment transactions, both online and offline, below certain thresholds, and in accordance with risk management rules that will be established.

Privacy is a fundamental right that allows individuals to develop their autonomy. The right to privacy is protected by international treaties and agreements, as well as legislation in Israel and around the world. Information collected during the operation of a payment system can reveal insights about individuals, such as their economic status, consumer behaviour, location, and even ideological preferences. Combined with data from other sources and advanced analytical capabilities, a comprehensive profile of the user can be derived. Given that payment systems typically generate relatively low profitability, there is an incentive for various service providers to leverage the existing information in the system for business purposes.

Prior to the issuance of the digital shekel, users face two extreme options regarding privacy: on one hand, with cash, payments are completely anonymous, and the means of payment itself does not retain any information about the users' identities or the payment transaction. This, of course, has advantages in terms of privacy protection, but it also raises significant

challenges regarding the prevention of money laundering and terrorist financing, and it supports the black economy. On the other hand, in digital payments or checks, the information collected during the payment transaction is stored and documented over time. Most existing payment systems were not initially designed with privacy in mind ("Privacy by Design") but rather implement principles and regulations that were given retrospectively. With the digital shekel, as a new payment system drawing from both the features of cash and those of digital means of payments, we have the opportunity to design the system optimally, ensuring that privacy principles are integrated into the system's technical features from the outset. This approach aims to balance the protection of user privacy with the need to prevent misuse of the system, such as tax evasion, money laundering, and terrorist financing (see section 7.4).

Beyond the fundamental right to privacy described above, end users may also seek privacy in a payment system to prevent the misuse of information about them (e.g., aggressive marketing) and to avoid unwanted tracking. In the case of CBDCs, there is often concern that they will be used by authorities to monitor the activity patterns of the public. As explained below, the privacy principles of the digital shekel system primarily address this concern.

The privacy design of the digital shekel is expected to provide a higher level of privacy than currently exists in advanced means of payments, but lower than that of cash. The Bank of Israel, in its various roles, as well as any other central entity, will not have the ability to access personal identifiable information about the activities of end users in the digital shekel.[81] This feature will be ensured technologically (by design), not just through regulation, as explained in detail in sections 6.1 and 6.2. Identifiable information about the activities of end users in the digital shekel system will be available only to system participants, particularly PSPs – each concerning their customers, similar to the current situation. If law enforcement authorities require personal identifiable information about the activity of any end user, they will do so through the participants and according to the law, similar to the current situation with other digital means of payments. The Bank of Israel will have aggregate information about system activity by sectors and defined segments, in the additional databases described in section 6.1. The possibility of shortening the duration for which participants are

[81] Unlike the information that will be available about participant activities – see section 6.1.

required to retain information about user activities compared to the current situation will be examined to enhance the level of privacy in the digital shekel.

The digital shekel will also allow for anonymous transactions, both online or offline. The system design will support the ability of an end user to perform a payment transaction to another end user without the PSP or any other entity receiving identifiable information about the payment transaction.[82] The decision on offering this feature, the relevant thresholds, the activity sectors for which it will be allowed, and other risk management mechanisms will be determined in regulation and/or relevant legislation.

The privacy rights of end users against system participants and in general will be determined according to GDPR rules, as far as they align with Israeli legislation. In any case, participants will not be able to use the information they accumulate about users and their activities in the digital shekel system for commercial purposes unless users give their clear and informed consent, which will be documented by the participant.

Box 5: The Level of Privacy in the Digital Shekel - Between Cash and Existing Digital Means of Payments

Several features interwoven in this section and other sections of the document validate the statement that the level of privacy in the digital shekel will be higher than that of existing means of payments, even if lower than that of cash:

The Mechanism for Message Transmission Between Participants: A transaction message in the digital shekel system will not rely on the configurations of existing payment systems, where typically the full message, including personal identifiable information, passes through the system operator (as is done, for example, in bank transfers through MASAV) or through another entity (for example, through SWIFT in the case of the RTGS system). If the transaction message passes through the backend layer it will do so in a way that the identifiable information is encrypted from it. Alternatively, the message can be transmitted in a two-way communication between the relevant participants themselves. This approach offers a higher

[82] A possible technology that can support this feature was examined in a technological experiment conducted by the Bank of Israel. For more details, see: Zafran, A., Mizrahi, T., & Soffer, Y. (2022). Experiment on a Distributed Platform. Bank of Israel.

inherent level of privacy ("by design") because, unlike existing payment systems, all the information contained in the messages, including personal identifiable information, will not be concentrated with by a single central entity.

The Information Included in a Transaction Message in the Digital Shekel System: The transaction message that passes through the system will only include the minimal information required regarding the end users involved in the transaction. The scope of the information included in the message can, of course, be influenced by the type of transaction (e.g., in the case of salary payments or cross-border transfers) and interoperability considerations, in cases where one leg of the transaction is not in the digital shekel system.

Participants' Use of Information: Participants will not be able to commercially use (monetise) the information of end users without the explicit and informed consent of the end users, all in accordance with the Privacy Protection Law.

The Period for Retaining Information by Participants: If, within the legislative process of the digital shekel, it is possible to reduce the period of legal exposure for participants in the system due to its unique characteristics (settlement in end users' wallets, finality, etc.), this could serve as a basis for defining a shorter period for retaining information regarding transactions in the system by participants.

Anonymous Payment Transactions: In anonymous payment transactions, no identifiable information will be retained by the participants, similar to the situation in a cash transaction. However, the end user may choose to retain information about their transactions on their personal device (without this information interfacing with the PSP systems).

Questions – Privacy:

65. Does the design proposed specification along the document align with the principles of "privacy by design"? Does it ensure that neither the Bank of Israel nor any other central entity will have the ability to access personal identifiable information about users' activities?
66. Is it important to allow anonymous transactions, both online and offline, in the digital shekel? Should this be allowed for all types of users?

67. Is it appropriate to allow participants to commercially use information about users only with the explicit consent of the user? How can this be ensured?

7.2. Cost of Using the Digital Shekel

The cost of using the digital shekel for basic activities should be low to negligible. Individual users will not pay fees for these activities. As the digital shekel is a public good, the Bank of Israel will bear the costs of managing and operating the system. PSPs will be able to charge a fee for receiving payments from merchants and will pay an interchange fee to the payer's PSP.

The public perception of cash is that its use does not involve any cost. This perception is not entirely accurate; withdrawing or depositing cash usually involves some cost, especially for businesses, and holding cash itself incurs costs, such as those arising from the risk of loss. Nevertheless, the cost of using cash is lower than that of digital means of payments, which is reflected in the fees charged to the public and especially to businesses. Moreover, the fees in digital means of payments are known and clear, whereas the costs of cash are sometimes less tangible.

As a digital natural extension of the physical cash issued by the Bank of Israel, it is desirable that the cost of using the digital shekel for basic activities be low to negligible. However, as a digital payment system where there are significant roles for participant from the business sector, the need for these participants to maintain a sustainable business model must be considered.

From the perspective that the digital shekel is a public good, the Bank of Israel will bear the costs associated with managing and operating the digital shekel system – the costs of managing the scheme, operating the backend layer, and additional services managed by the Bank of Israel, among others. This is similar to cash and different, for example, from the RTGS system, where the Bank of Israel charges participants for its operating and management costs. However, to maintain flexibility for future developments, the system will be built so that the Bank of Israel retains the option to charge various fees from participants. For this

purpose, the system will need to allow the Bank of Israel to distinguish between types of transactions (for example, the bank may decide to charge fees for business-to-business transactions but not for person-to-person transactions).

Section 3.3.1 describes the interchange fee mechanism that the PSP of a payee who is a business will transfer to the payer's PSP, and Box 1 in section 3.3.1 describes the services that PSPs will need to provide to end users, including the services they will need to provide without charging a fee. In particular, the box emphasises the package of mandatory free activities that a private end user will be entitled to, ensuring that the basic services of joining the system, funding the wallet, and performing basic payment transactions will be free for individual users. In general, the merchant fee for a simple payment transaction in the digital shekel will be lower than that customary for debit cards. The Bank of Israel, as the system manager, will be able to define the maximum fees for different transactions according to the type of transaction, and the system will allow these definitions to be enforced technically as well.

Questions – Usage Costs:

68. In defining the cost model for the digital shekel system, there is a tension between the desire for a product that mimics cash (with no direct cost) and the need for a sustainable business model for profit-oriented business sector participants. The design proposes a base layer model similar in nature to that existing in credit cards – a business fee and a cross-fee with no cost to the payer. Are there other models that can support a sustainable business model for intermediaries alongside zero/low cost for end users?
69. To what extent will the fact that the Bank of Israel bears the costs of managing and operating the digital shekel system contribute to the low cost of using the digital shekel?

7.3. Consumer Protection

Users of the digital shekel will receive consumer protection similar to that provided by other digital means of payments. PSPs will be responsible for preventing fraud and compensating customers in case of fraud, in accordance with the rules in the Payment Services Law.

Offline payment transactions and anonymous transactions will not be eligible for consumer protection.

Holding and using cash does not include any consumer protection. In cases of loss, fraud, failure to supply the good or service, etc., the user is not entitled to any protection or compensation from the Bank of Israel as the issuer of the currency or from any other entity in relation to the use of cash as a means of payment. However, in digital payment systems, there are rules for the responsibility of service providers and the rights of users, and as a digital payment system, the digital shekel system will be committed to providing comprehensive consumer protection to its users and maintaining the reliability and efficiency of the system. The purpose of consumer protection is to ensure a safe and reliable user experience that aligns with existing payment systems, to strengthen public trust in the system, and at the same time to maintain reasonable operating costs.

PSPs will bear the primary responsibility for consumer protection in the digital shekel system. They will be responsible for identifying and preventing fraud, as well as compensating users who have been harmed by misuse events. PSPs will be required to establish and operate advanced internal fraud detection and monitoring systems. They will also need to provide efficient customer service and a quick response to user complaints.

Alongside the digital shekel system, a central fraud monitoring system[83] will operate, supporting the PSPs. This system will assist in identifying and preventing fraud at the system level, using its ability to analyse unusual activity patterns from a broad perspective. The system will enable PSPs to receive alerts about suspicious activity, but it will not replace their internal systems nor reduce their responsibility towards end users. Combining the PSP's information with the information received from the fraud monitoring system will provide the PSP with the ability to form a holistic picture of the parties involved in the payment transaction.

The responsibility of payment service providers in the digital shekel system will be in accordance with the provisions of the Payment Services Law, which applies to financial service providers in the existing financial system. In particular, in online transactions, PSPs

[83] For more details, see section 3.2.2.

will provide full compensation to users in case of misuse, while in offline transactions, due to the inability of PSPs to monitor the activity in real-time, a user who chooses to perform an offline transaction will not be compensated if they fall victim to fraud. Anonymous transactions will also not be compensated as part of the consumer protection.

Questions – Consumer Protection:

70. Consumer protection involves operational burdens and costs for system participants. Is it appropriate to establish consumer protection in the digital shekel at a level not less than that of existing digital means of payments?
71. Is it appropriate to impose on PSPs the responsibility for consumer protection, fraud prevention, and compensating users harmed by misuse events? Would this be a significant barrier to entry for entities wishing to operate as PSPs? Are there alternative solutions?
72. Should ASPs also be required to bear responsibility for consumer protection?
73. Is it appropriate that anonymous transactions and offline transactions will not be eligible for consumer protection?

7.4. Anti-Money Laundering and Counter-Terrorism Financing

The Digital Shekel system must comply with anti-money laundering combating terrorism financing rules, using advanced technologies and methods to ensure its reliability and prevent financial crime. PSPs will bear the primary responsibility for risk management, including "Know Your Customer" processes, monitoring payments, and reporting suspicious activities. The system will be designed to comply with international anti-money laundering standards, with mechanisms for information sharing between PSPs to meet regulatory requirements.

As a digital payment system, the digital shekel system must comply with anti-money laundering and combating the financing of terrorism rules and adopt the most advanced

technologies and methods in this field to ensure its reliability and to ensure that it does not support crime in general and financial crime in particular.

PSPs will bear the primary responsibility for managing AML and CFT risks in the system. They will conduct "Know Your Customer" processes and due diligence checks for new system joiners. They will monitor payments according to the guidelines of the system manager and the Money Laundering and Terror Financing Prohibition Authority (IMPA) and make the required reports by law, including on suspicious activities. To fulfil their responsibility, PSPs will use real-time monitoring systems and will be required to keep detailed records of transactions. It should be emphasised that although transactions in the digital shekel will be immediate as described in section 4.5, a PSP can delay the execution of a transaction to perform the necessary monitoring and even refuse to complete it, if the transaction is found to be suspicious (and if the user does not satisfy the PSP regarding its legitimacy), this is true both on the payer's and the payee's side. Privacy-enhancing technologies (PET) will allow monitoring of transactions while maximising user privacy.

Funding and defunding processes from an account at an FI will be monitored, as necessary, by both the PSP and the FI, both of which serve the customer and know the nature of their activities. In funding and defunding against cash, especially when performed at an ATM or an FI counter where the end users does not have an account, the responsibility for monitoring the transaction will lie with the PSP.

ASPs will not be required to conduct a "Know Your Customer" processes and will not bear responsibility for managing AML risks, as ultimately the payment transactions resulting from the advanced payment applications offered by ASPs will pass through the PSPs, who will perform the monitoring as with any payment transaction. However, ASPs will be required to ensure that the services they provide do not facilitate illegal activities (e.g., cases where a customer initiates payment transactions through an ASP to be performed by different PSPs, which if performed by a single PSP would require AML checks by the PSP).

Since different participants in the system may be supervised by different regulators, it is important to establish uniform standards for AML requirements for all participants in the system to prevent regulatory arbitrage. Together with the system manager, IMPA is expected to play a central role in providing professional guidelines for designing rules and standards

in this area, such as rules for onboarding users to the system, minimal documentation in a uniform format, declarations about the sources of funds, the type of user activity, the ownership structure in business accounts, and aspects of cooperation and information sharing between participants.

If the system allows for anonymous payment transactions, where PSPs are not exposed to information about the characteristics of the transaction, its amount, and the participating parties (see section 7.1 Privacy), limits and thresholds for these transactions will be defined to minimise the risk of money laundering and terrorist financing.

As described in section 5.1.2, the digital shekel will be designed to comply with international AML standards. A mechanism for information sharing between PSPs will be implemented to meet the Travel Rules requirements in cross-border transactions, ensuring compliance with FATF[84] standards and other international regulations.

Questions – Anti-Money Laundering:

74. Is it appropriate to impose on PSPs the responsibility for managing AML and terrorist financing risks in the system, similar to existing payment systems? Would this be a significant barrier to entry for entities wishing to operate as PSPs? Are there alternative solutions?
75. Given that funding and defunding against cash, the FI will not be exposed to information about the end user, should it be exempt from responsibility for managing AML and CFT risks in these processes, placing the responsibility solely on the PSP?
76. Can central components be added to the system to assist participants in managing AML CFT risks without reducing the participants' responsibility in this area?
77. How can AML and CFT risks arising from anonymous transactions be managed?

[84] In particular, Recommendation 16, which deals with the transfer of information during a payment transaction.

7.5. Information Security in the Digital Shekel System

The Digital Shekel system will be designed and built to high standards to ensure data integrity, user privacy, and protection against threats. The system manager will define policies and procedures for managing system security, while participants will be required to meet stringent standards and conduct independent audits. The system will be designated as critical national infrastructure and will comply with the standards of the National Cyber Directorate.

Information security is a critical component of any payment system, especially a national system operated by the central bank, which must gain the trust of the general public to achieve its intended goals. The digital shekel system will be designed and built with high standards of information security to ensure data integrity, user privacy, and protection against external and internal threats.

The digital shekel system manager will define policies and procedures for managing system security. They will be responsible for managing the security risks of the entire system, while the system operator and participants will manage the security risks of their systems according to the manager's requirements. The system manager will define cybersecurity standards that will apply to the system operator and participants and will require them to demonstrate compliance with these standards through independent audits. These audits will be conducted by external and independent entities to ensure their reliability and accuracy. In addition to these audits, the manager will have the right to conduct independent audits of the operator and participants as needed. These audits will allow the manager to ensure that the system operates according to the highest standards of information security and that participants meet the stringent requirements. Additionally, the cybersecurity unit at the Bank of Israel will be responsible for securing the backend layer and additional services managed by the Bank of Israel. It will employ experts and professionals who will focus on securing the digital shekel, gather relevant security intelligence, and analyse all threats and aspects related to the system's cybersecurity.

The digital shekel system operator will establish, monitor, and maintain KPIs and key risk indicators (KRIs) for the cybersecurity of the digital shekel. These metrics will allow the system operator and system manager to track security performance and identify potential

issues in real-time. The system will be designated as critical national infrastructure and will comply with the standards and guidelines of the National Cyber Directorate. The system manager will ensure that its standards are aligned with the Directorate's requirements, and the system operator and participants will ensure that their systems and services meet these standards.

Participants in the digital shekel system will be required to be certified under an appropriate cybersecurity framework or standard, such as ISO 27001. The system manager will define the minimum scope and applicability of each such certification. These certifications will ensure that participants operate according to the highest standards of information security and take all necessary measures to protect their information and services.

The system operator and participants will use preventive and detection security controls that will allow them to identify and address attacks from significant adversaries. These controls will include strong authentication, strong encryption and key management, secure communication, high system redundancy, and protection of external endpoints. These controls will ensure the confidentiality, integrity, and availability of services. The system will be designed to handle advanced threats and ensure the highest level of security.

The system operator and participants will implement controls appropriate to the risks the system will face. These controls will include the most advanced technologies and procedures, at least similar to those implemented in other national payment systems. These controls will include technical, organisational, and physical measures to ensure the confidentiality, integrity, and availability of services.

The system operator and participants will assess and monitor the security and fraud risks to their systems and services and implement controls to mitigate these risks. These controls will include measures to prevent unauthorised or unintended use of systems and services, as well as measures to detect such use. The system will be designed to handle advanced threats and ensure a very high level of security.

Questions – Information Security:

78. Are the information security risks associated with the digital shekel, as described in the document, significantly different from those in existing payment systems?
79. Should the system manager define information security requirements within the rules, or rely on the information security requirements set by the regulators overseeing the participants? How can the manager ensure participants' compliance with the established requirements?

7.6. Holding Limits to Prevent Harm to the Stability of the Banking System

To hedge risks to the liquidity of the banking system and adverse effects on the supply and price of credit, there may be holding limits on the balances of end users in the digital shekel, and in case of a crisis, also funding limits. These limits will be set considering the impact on the user experience and the need for flexibility to adapt to public adoption and long-term effects.

Preliminary simulations for calculating the holding limits required for different types of users indicate that the holding limits will not constitute an effective barrier in most use cases. Use cases that require exceptionally high amounts will be facilitated by mechanisms that maintain a smooth and convenient user experience alongside the holding limit regime.

The conversion of bank deposits to digital shekels is equivalent from the banking system's perspective to cash withdrawals, as both cash and digital shekels are not part of the banking system's balance sheet or its sources of funding when held by the public. Additionally, the digital shekel includes unique features not present in cash due to its digital, including ease of holding, use, and conversion from deposits in the banking system. These features present

a new potential risk to the banking system's sources of funding and liquidity, and consequently to the economy, due to the possible impact on the supply and price of credit.[85]

The potential risk to the banking system from the possible issuance of a digital shekel can be divided into two main categories: 1) Immediate risk to the system's liquidity or to an individual bank due to a rapid shift by the public to the digital shekel. For example, immediately after its issuance and the public's familiarity with it, or in case of concerns about the stability of the banking system or even the stability of an individual bank, which may lead customers to take advantage of the ease of conversion to the digital shekel and withdraw their deposits in significant volumes. 2) Ongoing risk to the composition of the banking system's funding sources, which would lead to a reduction and/or increase in the cost of credit supply in the economy, as public deposits are the cheapest sources for the banking system. The principles presented below are intended to hedge the potential risk from the possible issuance of a digital shekel, with an emphasis on the banking system's liquidity aspects and hedging the immediate risk as a basis for managing the ongoing risk as well.

According to the literature, several tools can hedge the risk: limiting the amount or number of transactions that end users can perform within a certain period, applying a negative interest rate above a defined holding threshold,[86] and more. One of the most effective tools for limiting this risk is imposing holding limits on the balances of end users in the digital shekel system. A holding limit regime allows for efficient hedging of liquidity risk and the risk of harm to banking intermediation.[87] On the other hand, such a regime adds business and technological complexity in building the system and may also harm the user experience if designed without considering the needs of different types of users and the various use cases the digital shekel system intends to support.

To address the tension between risk mitigation and potential impact on user experience in the system, the negative effects of holding limits on user experience and the public's interest in using use the digital shekel will be considered. Additionally, the Bank of Israel will have

[85] For more details, see: Buchholz, Z., Michelson, N., Ettinger, B., & Soffer, Y. (2022). Possible Effects of a Digital Shekel on the Banking System. Bank of Israel.

[86] Presenting a possible model, especially for periods when the interest rate in the economy is very low: Panetta, F., & Bindseil, U. (2020). Central bank digital currency remuneration in a world with low or negative nominal interest rates. VoxEU Column Monetary Policy.

[87] "Disintermediation"

the flexibility to make changes to the holding limits in response to actual public adoption and usage of the digital shekel, taking into account the long-term effects on the Israeli economy in general and on the banking system in particular, with an emphasis on the supply and cost of credit. Furthermore, while risk mitigation will be based on holding limits, the Bank of Israel will also have the option to impose funding limits[88] as an immediate response to concerns about a possible crisis in a specific bank or a systemic crisis.

Table 6 – Examples of System Challenges in Implementing a Holding Lomits Regime and Possible Mitigation Approaches

Solution	Challenge
Impossible to receive amounts above the holding limit.	**Waterfall** – Automatic defunding of the excess amount (or more) to a connected FI account.
Need to perform frequent funding due to the limit.	**Reverse waterfall** – If there is insufficient money in the wallet to perform a transaction, an automatic funding to the wallet from a connected FI account of the missing amount (or more) will be performed.
Need to know the user's total balance in the case of multiple wallets for a user.	**Central system** – Which will connect all the user's balances across all their wallets without exposing their identity, allowing the enforcement of the holding limit.
Difficulty in offering the option for shared wallets.	Possible solution at the PSP level.

An **initial** model to calculate the required holding limits for different types of users (private and various sizes of businesses) based on defining a possible shock to the banking system's liquidity coverage ratio (LCR)[89] and considering different scenarios regarding public adoption of the digital shekel suggests the magnitude of the limits that will need to be set.

[88] A funding limit restricts the amount an end user can fund into the wallet within a given period, regardless of the wallet balance at that time.
[89] LCR - Liquidity Coverage Ratio

The model calculates five levels of holding limits according to the supervisory activity sectors used in the banking system[90]– for individuals (private end-users), and for micro, small, medium, and large businesses, based on the population size in Israel and the number of active businesses in each activity sector. The ratio between the monthly expenditure size for individuals and the revenue of businesses in credit cards served as an initial basis for defining the multipliers required between the holding limits for individuals and those for businesses of different sizes, while considering the desired duration in each segment for activity in the digital shekel without needing to fund or defund the wallet against a bank account – one month for individuals up to small businesses, one week for medium businesses, and one day for large businesses. The preliminary simulations in the model assume moderate adoption of the digital shekel by the public and a willingness to absorb a moderate impact on the liquidity coverage ratio of the banking system. In such a scenario, the model results based on 2024 data show that the magnitude of the required holding limits will allow end-users – individuals, as well as businesses of all sizes, to operate in a wide range of use cases without the holding limit being a binding constraint on activity. This includes use cases of not every-day payments (such as most payroll payments in the economy and common business-to-business transactions), The results should be taken with the necessary caution due to various factors, including the novelty of the model, the need to update the baseline data regarding the banking system metrics and potential number of digital shekel users close to the implementation of the holding limit regime, improvements and refinements to the model down the road, and the need to examine the impact on individual banks as well. However, the results allow for an initial assessment that the impact on the user experience in most reasonable use cases due to the implementation of the holding limit regime is expected to be insignificant. It should be noted that waterfall and reverse waterfall mechanisms allow for the making and receiving payments even beyond the holding limit thresholds.

The magnitude of the limits obtained in the model may still restrict the development of advanced use cases involving the locking of large amounts for limited periods – for example, for financial asset trading purposes. Therefore, mechanisms that allow for holding beyond

[90] For the simulation, we used these data, but the model can accommodate any other segmentation decided upon.

the limit for a limited period based on predefined criteria will be examined – for example, allocating exceptions to participants who will allocate them to their customers, a model of paying for temporary exceptions to the limits, or other models.

Questions – Holding Limits:

80. Are holding limits the best way to address the risk to the banking system inherent in the issuance of a digital shekel, despite the potential impact on user experience and the operational complexity involved in implementing them?
81. What complexities can arise from differential holding limits based on the type of user?
82. What should be the holding limit for different types of users (private user, small business, large business, etc.) to ensure that the user experience is not compromised while mitigating the risk to the banking system? What criteria should be used to calculating these limits?
83. What mechanisms can be implemented to allow the locking of amounts exceeding the holding limit for limited periods, for example, for financial asset trading purposes?

7.7. Interest Payment to End-Users in the Digital Shekel

The Digital Shekel system will enable the functionality of paying interest on the held balance, which can enhance monetary transmission and competition in the deposit market. Paying interest may affect bank stability, change the perception of the digital shekel as a means of payment, and create additional costs for the Bank of Israel. The decision on paying interest and its rate will be at the discretion of the Bank of Israel based on monetary and macroeconomic conditions, considering the associated risks and complexities.

The digital shekel system will enable a functionality for the Bank of Israel to pay interest on the balance held in digital shekels directly to end users. Three main advantages can be identified for this capability:

1. **Enhancing the Monetary Transmission**: When the Bank of Israel raises the interest rate, this change does not fully and immediately pass through to households and most businesses. An interest-bearing digital shekel has the potential to accelerate the transmission of monetary policy, especially regarding the deposit rate. For example, during the interest rate hikes in 2022-2023, it became increasingly clear that the banking margin changes with interest rate changes. In particular, the interest rate on credit changed quickly and with high correlation to the Bank of Israel's rate, while the interest rate on deposits, especially short-term, adjusted slowly and only partially. Additionally, the interest rate on current account deposits mostly remained zero, while the overdraft interest rate increased fully and immediately. Paying interest on the digital shekel aligned with the policy rate may incentivise banks to retain deposit funds and raise their interest rates more closely aligned with the Bank of Israel's rate. The Bank of Israel will gain a tool to enhance monetary transmission, improving the mechanisms through which the policy rate affects macroeconomic aggregates such as prices, employment, and output.
2. **Increasing Competition in the Deposit Market**: As a result of the process described above.
3. **Enhancing the Attractiveness of the Digital Shekel**: Paying interest will increase the incentive for users to hold digital shekels, which may also increase its usage. However, this is not a sufficient reason to decide on paying interest, as public demand for the digital shekel is expected to come from the benefits it offers, as described in the introduction to this document, rather than from a financial incentive offered by the Bank of Israel.[91]

On the other hand, the decision to pay interest on the digital shekel also entails many risks and complexities:

1. **Impact on Bank Stability**: High demand for the digital shekel may lead to the transfer of deposits from banks to the digital shekel, potentially harming bank

[91] When there are economies of scale (in this case resulting from a network effect), there is theoretically justification for some subsidy, especially in the initial stages. However, even if such an incentive is decided upon, it is expected to be temporary and not necessarily in the form of interest payment.

stability and profitability. Banks may raise deposit interest rates to cope with the situation, but this could reduce their profitability and increase the cost of credit in the economy. However, this risk can be hedged by limiting the maximum amount for which interest will be paid on the digital shekel, so it is lower than the holding limit set according to the parameters described in section 7.6.

2. **Public Perception of the Digital Shekel**: Positive interest may cause the digital shekel to be perceived more as a store of value and less as a means of payment, potentially harming its usability as a means of payment.
3. **Cost**: If the digital shekel replaces bank deposits, interest on the digital shekel that is lower than the Bank of Israel's rate will reduce the Bank of Israel's interest payment costs. If the digital shekel replaces cash, on which the Bank of Israel does not pay interest, paying interest will create a cost for the Bank of Israel.
4. **Financial Inclusion and Distributive Justice**: Interest on the digital shekel may disadvantage certain populations that do not use digital technology. However, the risk of this is low as the digital shekel will be designed to be suitable for all populations.
5. **Perception of Privacy**: The architecture presented in this document emphasises privacy protection and allows for interest payments from the Bank of Israel to users without the Bank of Israel knowing who the interest recipient is. However, the public may find it difficult to understand the mechanism, and the perception of the digital shekel's privacy may be affected.
6. **Calculation and Frequency of Interest**: Since digital shekel payments are immediate and final 24/7/365, the digital shekel does not have a business day. It must be determined how and when to calculate and pay the interest, which may create technological challenges and arbitrage opportunities.
7. **Multiple Wallets**: Since each user can hold more than one wallet with more than one PSP if the interest is tiered,[92] the calculation should be done on all the user's wallets. This is a technical complexity that requires a central solution, like the one proposed for holding limits (section 7.6).

[92] For example, positive interest from zero shekels up to a certain ceiling, and zero interest above this ceiling.

The digital shekel will be designed so that, technologically, it will be possible to pay interest on the digital shekel at a rate determined by the Bank of Israel (which will in any case be lower than the Bank of Israel's rate) only to a specific activity sector (at this stage, it seems appropriate to consider this for the private users and micro-businesses sector in Israel), up to a limited holding threshold that will be equal to or lower than the holding limit, and without the Bank of Israel or any other central entity having specific information about the interest receipts of any user. If the interest payment raises the wallet balance above the holding limit, a waterfall mechanism will be activated, or the payment will be deferred until the balance in the wallet is can accommodate it. Regarding tax on interest income – one option is that it will be deducted at source by the system operator, while the PSP will provide a service of reporting interest income similar to how banking corporations do today, so the user can offset this interest against capital losses or financing expenses when eligible. It should be emphasised that the interest will be credited directly to the user's wallet (and only to an online wallet – no interest will be paid on offline digital shekel balances), and the interest funds will not pass through the PSP's wallet in any form.

The decision to activate or stop the interest payment mechanism and its rate will be at the discretion of the Bank of Israel based on monetary and macroeconomic conditions, and the level of competition in the financial sector at any given time, considering all the risks described above.

Questions – Paying Interest:

84. Is it appropriate for the Bank of Israel to pay interest to holders of the digital shekel, specifically for households and micro-businesses?
85. What risks and complexities arise from paying interest on the digital shekel that are not described in the section?
86. How frequently should interest payments on the digital shekel be made? What implications could the frequency and timing of interest payments have?

8. Summary and Next Steps

The issuance of the digital shekel, if decided upon, will represent a significant transformation in the financial system in general and the payment system in Israel in particular. It has the potential to offer numerous benefits to the Israeli economy and the end-users who adopt it. However, it is important to recognise that this is a complex initiative that also involves substantial risks. This document, the result of a prolonged and in-depth design effort, was written with the aim of designing the digital shekel to deliver the expected benefits while deeply considering the associated risks and how they can be mitigated.

This document represents a preliminary design, and even if a decision were made now, it does not encompass everything necessary to enable the issuance of a digital shekel at this stage. Building the digital shekel system will require a more detailed design than what is presented here, and several significant processes will need to be carried out to implement it. Various aspects of the design, as well as ensuring the Bank of Israel's legal authority to issue a digital shekel according to this design, will likely necessitate legislative processes. Additionally, the design outlined in this document provides roles to a wide range of entities beyond the Bank of Israel, including government ministries, financial institutions, financial infrastructure providers, international entities, and more. To implement the design, all these entities will need to cooperate in the construction and operation of the digital shekel. Some of these entities are already regularly participating in the project's public consultation forums, which are held quarterly.[93] It will also be necessary to thoroughly examine the available technologies for implementing the design and ensure that it can indeed be executed from a technological perspective. If the decision is made to issue the digital shekel, a significant public awareness campaign will be essential to introduce the new means of payment to the general public.

With the completion of the preliminary design, the digital shekel project is moving to the next phase, and in the years 2025-2026, the project will focus on the following topics:

[93] Bank of Israel, Digital Shekel Project - Financial Industry Forum. (Link only available in Hebrew).

- Comprehensive economic analysis of the costs and benefits, opportunities, and risks associated with issuing a digital shekel. This analysis should consider both the project cost and the broader economic impact, alongside the potential to enhance efficiency and innovation in the payment system. As part of this, the implications for financial intermediation in the economy will continue to be examined.
- Learn and deepen familiarity with the available technologies for implementing the design, while continuing to conduct technological experiments as needed.
- Adapt the design based on feedback received on this document, public preferences as revealed by studies conducted by the project[94], and the results of the technological and economic analysis.
- Prepare for the legislative process. The bank will consider the possibility of parallel legislation to ensure the status and acceptance of cash.[95]
- Plan the regulatory framework in which the digital shekel will operate and the regulations that will apply to the various participants in the system.
- Thoroughly examine the implications of wholesale CBDC and the ability of the digital shekel to function as a multi-purpose CBDC[96] – meaning it can serve as both a retail CBDC and a wholesale CBDC.
- Prepare a roadmap for the possible issuance of a digital shekel. This includes prioritising components, users, and use cases, organisational planning regarding the various functions that will need to be established within and outside the Bank of Israel, procurement planning, deciding on conducting pilots in different areas before full launch, and more.
- Prepare a document that will recommend to the Governor of the Bank of Israel whether to decide to issue a digital shekel. This document will be written towards the end of the two-year plan, i.e., towards the end of 2026, based on all the processes described above as well as the status of the various indicators that the Bank of Israel has been monitoring since the publication of the document "Possible Scenarios for a Decision on the Issuance of a Digital Shekel".[97] Such a decision should primarily be

[94] Such as Plato Shinar et.al, 2024.
[95] Similar legislation – allowing the issuance of a digital euro while ensuring the status of cash – is currently being promoted in the European Parliament.
[96] As described in Box 2.
[97] Moshe, A., & Ribon, S. (2023). Potential Scenarios for a Deciding to Issue a Digital Shekel. Bank of Israel.

made by the Governor. However, since the issuance of the digital shekel according to the design presented in this document will likely require legislative changes, such a decision, if made, will ultimately need to be made in cooperation and with the support of the government and the Knesset.

This document is now being published to the public to present all stakeholders with the design that has been developed so far and to receive their feedback. At the beginning of the document, the section "How You Can Influence the Design of the Digital Shekel," outlines the manner in which stakeholders are invited to comment on the design in its various aspects.

References

1. Bank for International Settlements, & Group of Central Banks. (2021). *CBDCs: System design and interoperability*. Link

2. Bank for International Settlements, Bank of Israel, & Hong Kong Monetary Authority. (2023). *Project Sela: An accessible and secure retail CBDC ecosystem*. Link

3. Bank for International Settlements. (2023). *Annual report 2023*. Link
4. Bank for International Settlements, Bank of Israel, Norges Bank, Sveriges Riksbank, & BIS Innovation Hub Nordic Centre. (2023). *Project Icebreaker: Breaking new paths in cross-border retail CBDC payments*. Link
5. Bank for International Settlements. (2024). *Project Mandala: Streamlining cross-border transaction compliance*. Link

6. Bank of Israel (2018). The Team for the Study and Examination of Central Bank Digital Currencies – Final Report. Link
7. Bank of Israel (2021). The Digital Shekel of the Bank of Israel: Possible Benefits, Draft Model, and Issues for Examination. Link
8. Bank of Israel - Currency Department (2023). "Currency Department Review for the Years 2020-2022". Link
9. Buchholz, Z., Michelson, N., Ettinger, B., & Soffer, Y. (2022). Possible Effects of a Digital Shekel on the Banking System. Bank of Israel. Link

10. Di Iorio, A., Kosse, A., & Mattei, I. (2024). Embracing diversity, advancing together-results of the 2023 BIS survey on central bank digital currencies and crypto. Link
11. Elwell, C. K. (2011). Brief history of the gold standard in the United States. Link
12. G7 (2021). *Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)*. Link

13. Kantar Public. (2022). *Study on new digital means of payments*. Link
14. Miedema, J., Minwalla, C., Warren, M., & Shah, D. (2020). *Designing a CBDC for universal access* (No. 2020-10). Bank of Canada. Link

15. Moshe, A., & Ribon, S. (2023). Possible Scenarios for the Decision to Issue the Digital Shekel. Bank of Israel. Link

16. Panetta, F., & Bindseil, U. (2020). *Central bank digital currency remuneration in a world with low or negative nominal interest rates*. VoxEU Column Monetary Policy. Link

17. Panetta, F. (2021). Central bank digital currencies: a monetary anchor for digital innovation. *Speech at the Elcano Royal Institute, Madrid*. Link

18. Panetta, F. (2022). Demystifying wholesale central bank digital currency. *ECB Speeches*, *26*. Link

19. Plato-Shinar, R., Maman, L., Shema Zaltokrilov, R., & Yaacobi, N. (2024). The willingness of the Public to Adopt a Digital Shekel. Bank of Israel. Link

20. Zafran, A., Mizrahi, T., & Soffer, Y. (2022). Experiment on a Distributed Platform. Bank of Israel. Link (Link only available in Hebrew)