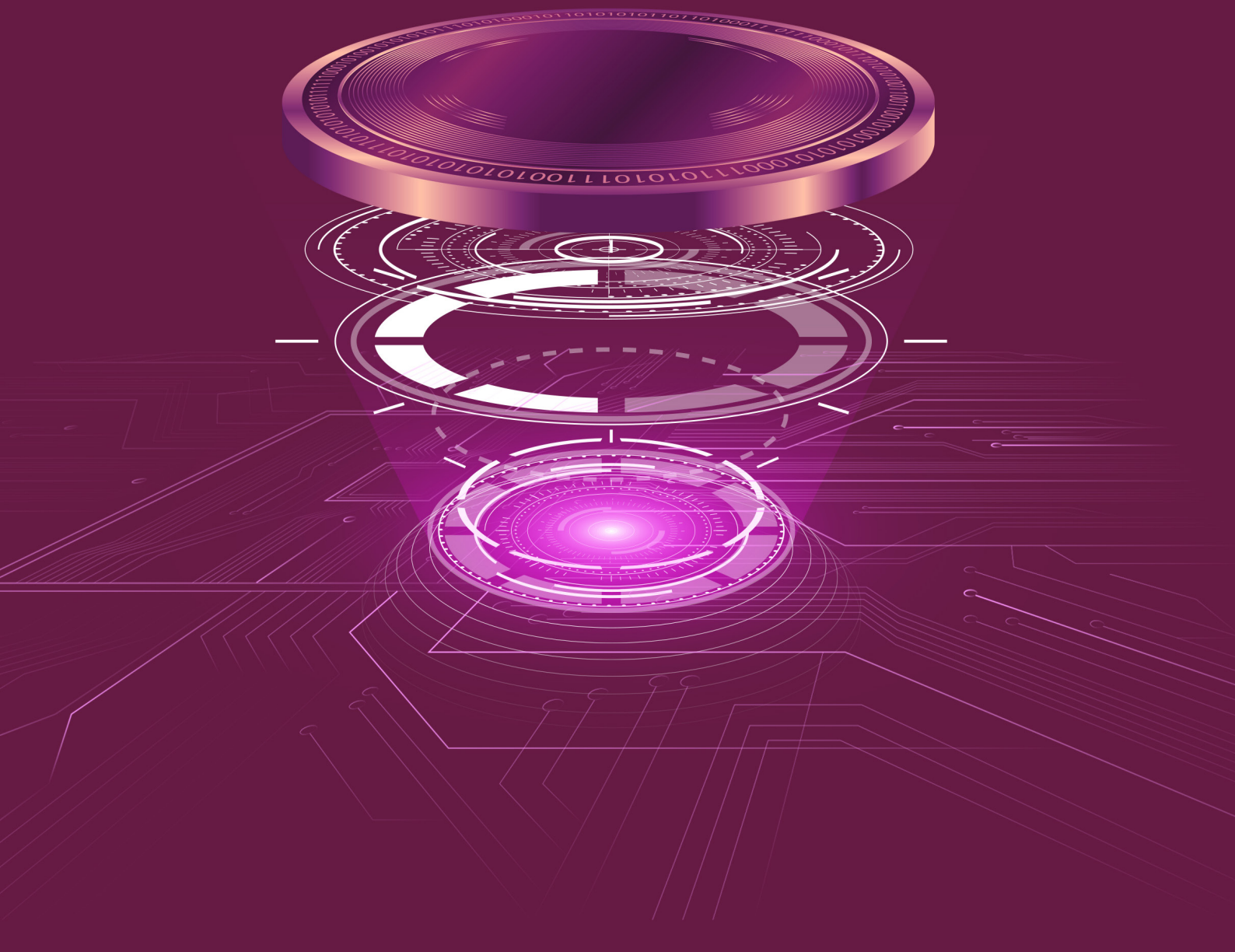
MINSAIT | BANCO DE ESPAÑA
Eurosistema

The Future of Digital Money: Digital Tokens and Wholesale CBDC Experimentation Program

Collaboration between the Bank of Spain and Minsait (Indra Group).
Final Report 2025



Summary

01

This document reflects the process of exploration and subsequent analysis of the possibility of integrating a wholesale Central Bank Digital Currency (hereinafter, wCBDC) into traditional settlement and payment processes, leveraging distributed ledger technologies (hereinafter, DLT).

The collaboration[1] between the Bank of Spain and Minsait-Indra aims to carry out an experiment to understand the impact that this wCBDC could have on the efficiency, security and agility of the financial infrastructures that process wholesale market operations.

Throughout the document, the different proposed use cases are analyzed, focused on the simulation of the issuance, distribution and settlement of a wCBDC, as well as its interaction with tokenized assets. The analysis identifies both potential benefits, such as the reduction of operating costs and settlement times, as well as some technical challenges involved in its implementation.

Based on the results of the experiment, this report offers key conclusions on the feasibility of integrating a wCBDC into current wholesale payment infrastructures, providing critical information for future strategic decision-making.

1- Collaboration agreement between Minsait and the Bank of Spain, published in the Official State Gazette, provision 9112, nº 110, 6 May 2024.

Introduction: Description and objectives of the Program

02

Background

The Experimentation Program on the use of Digital Tokens arises in the context of the growing initiatives led by Central Banks to explore the potential of digital currencies, in particular wholesale Central Bank Digital Currencies. At a global level, these initiatives seek to improve efficiency, agility and security in financial infrastructures that process high-value transactions, both payments and securities settlement.

The Bank of Spain, as part of its responsibility to promote the proper functioning of payment systems and in line with international trends, launched in December 2022 an experimentation program to evaluate the use of digital tokens in the settlement of wholesale transactions. Within this framework, the Bank of Spain has established an agreement with Minsait, with the aim of carrying out experiments focused on the integration of a wCBDC into DLT-based settlement platforms.

Description

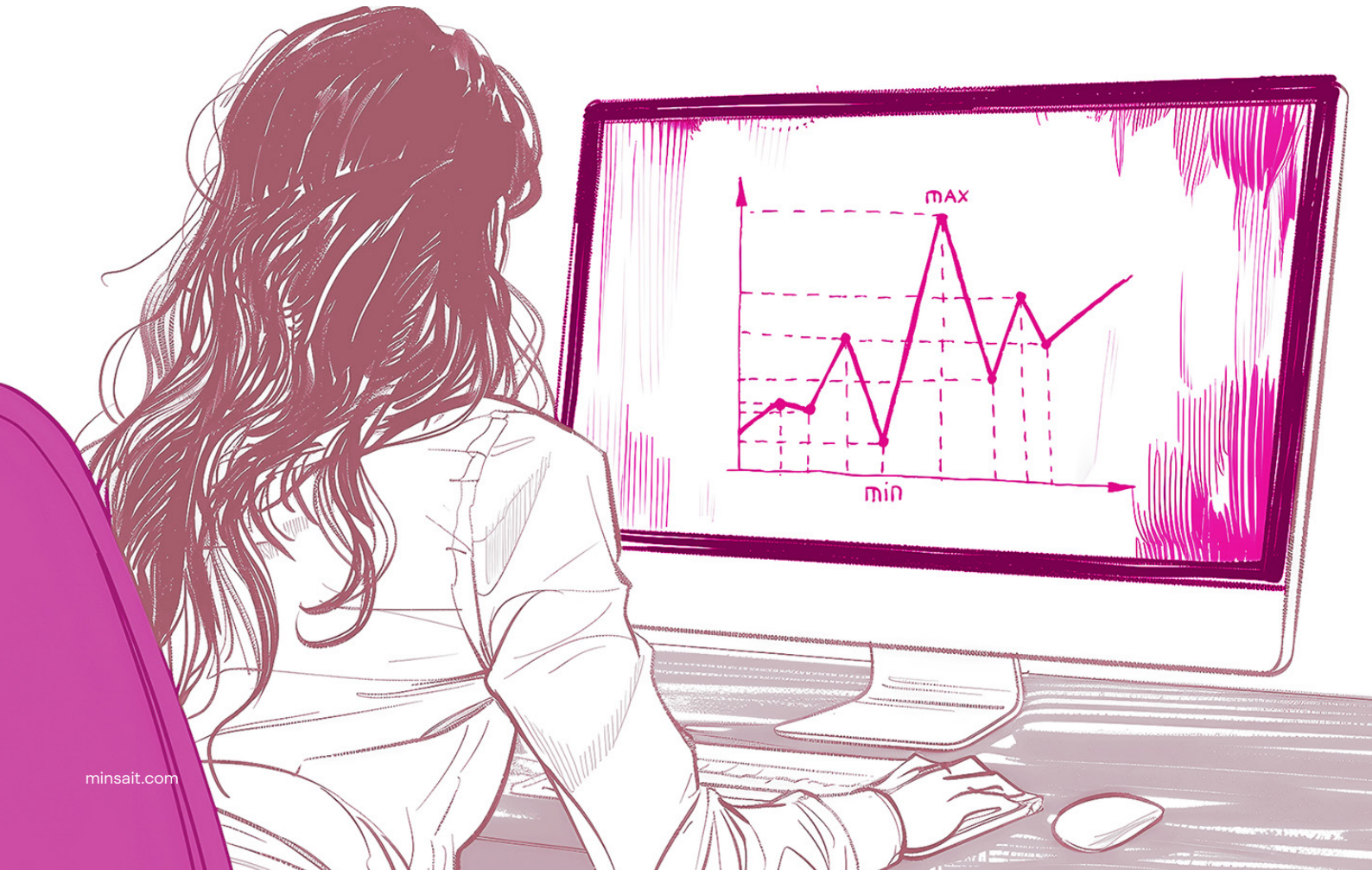
The Program focuses on experimentation with the issuance and settlement of digital tokens representing financial assets on a DLT platform, in combination with a wCBDC issued by the Central bank. To carry out the experimentation, different use cases related to the life cycle of a bond are proposed and the program is divided into phases of organization, design, construction of the prototype, experimentation and preparation of the conclusions report.

Objectives

The experimentation focuses on two dimensions: testing the integration of a wCBDC with the settlement of digital asset tokens on a single DLT platform ensuring an atomic settlement of the operation, and delving into the specific details about the implementation of a wCBDC and providing practical evidence on the possible advantages or disadvantages of the introduction of a wCBDC with respect to processes, traditional procedures and infrastructures and identify possible areas for improvement in current settlement processes.

Evaluation of use cases

03



3.1 Description of each use case and its design in DLT (Distributed Ledger Technology)

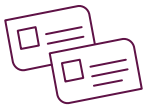
A proposal was made of different use cases ranging from the creation, issuance and distribution of a wCBDC, to the creation, issuance and redemption of a bond, thus covering the complete life cycle of said bond. For the correct development of these use cases, a platform based on DLT technology was created that allows the viability of the proposed cases to be evaluated.

This prototype has several Smart Contracts that have allowed the creation of tokens, the association of wallets and the transfer of tokens between different Participants. Role management has also been established in which permissions have been attributed to the different actors on the platform.

One of the needs of the business was the separation of two “legs”:

The cash leg

Where Central banks and Commercial banks intervene and cash tokens representing the wCBDC are traded.



The Securities Leg

Where CSD and Participants intervene and bond tokens are traded

In order to be able to obtain greater detail of the transactions carried out within the platform, a transaction explorer has been implemented, which gives greater visibility of the data obtained by the Smart Contract when a transaction is made. Blockscout is a Blockchain explorer for Ethereum that allows users to view, search, or verify transactions.

It allows you to obtain the detail of the contract to which the call has been made to execute the transaction, balances and performance data of the platform can be consulted.

Digital Money Issuance (Conversion)

The issuance and distribution of wCBDC is simulated, wherein a Central Bank issues wCBDC tokens on the platform and distributes them to Commercial banks through a smart contract based on Ethereum's ERC-20 standard. The following illustration shows some of the functions and events that the contract generates.

SMART CONTRACT	Required Functions		Events
ERC 20	Total Supply	Balance	Transfer
	Transfer	Approve	Approval
	Transfer from	Allowance	

Own creation

There are **three roles** in this use case:

Operator	In charge of creating the ERC-20 Smart Contract and registering the Central banks
Central banks	Issue new wCBDC tokens, create Commercial banks, and distribute the created tokens to them
Commercial banks	Receive wCBDC Tokens

Central banks and Commercial banks have cash wallets in which they can store wCBDC tokens. The information in these wallets is stored in a database. Some validations have been implemented when creating Commercial banks, which will have to be manually verified by simulating some of the KYC controls, in this way we achieve a simplified process that keeps the focus on the objective of the experiment and allows balancing between a minimum level of compliance and avoids an unnecessary burden of complexity.

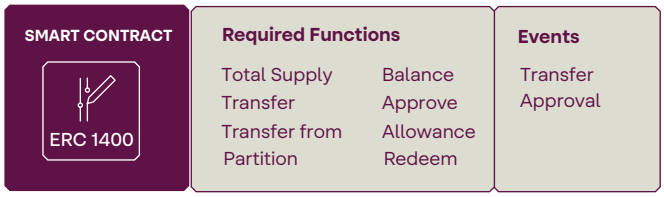
Issuance of a bond

In this use case, the process of issuing and settling a bond is simulated using Smart Contracts and ensuring an atomic settlement of the operation, i.e. the simultaneous transfer of wCBDC tokens and bond tokens. The issuance process encompasses the creation of Central Securities Depositaries (CSDs), the creation of the Participants who subscribe to the issuance, the association of Participants and Commercial banks to manage the settlement of the operation with wCBDC and the creation of Smart Contracts by the Operator. CSDs are responsible for managing the life cycle of the bond, from its creation to its redemption and corresponding "token burn". Bond issues have not been limited to an 'all or nothing' basis but have been designed in such a way that a partial subscription of the issue is possible. This is achieved thanks to Smart Contracts, which due to their flexibility and programmability allow the inclusion of functionalities that could facilitate a more dynamic market access adapted to the needs of the investors.

The objective is to settle the issuance of a bond with money from the Central bank. To this end, an association is made by means of a smart contract in which a Participant establishes a link with a Commercial bank, allowing the Participant to acquire the bond tokens while the Commercial bank is responsible for settling the cash leg associated with the operation, transferring to the Commercial bank placing the issuance the amount of wCBDC tokens corresponding to the number of bond tokens acquired by the Participant.

The smart contract that is responsible for associating the bond wallets of the Participants and the cash wallets of the Commercial banks is called Smart Contract Wallets Link, the smart contract that represents the bond token is based on the ERC-1400 standard, the smart contract that manages the registration of the Participants to the issuance is called Smart Contract Securities Manager and the smart contract that locks the wCBDC tokens and The bond tokens to perform atomic settlement is called Smart Contract DVP.

The following illustration shows some of the main functionalities of the ERC-1400 standard, which is an extension of the ERC-20 standard.



Own creation

The roles found in this use case are as follows:

Operator	In charge of creating Smart Contracts, registering CSDs and managing Smart Contract permissions
CSD	Register the Participants, create the bond tokens and issue the bond
Participants	They register for the bond issue and acquire the bond tokens in their wallets
Commercial banks	They settle the cash leg and the issuing bank receives the tokens in its cash wallet

Delivery versus payment of a bond

This use case simulates the Delivery vs Payment process, in which a Participant transfers bond tokens to another Participant. To carry out this process, a flow has been implemented in which Participant who wishes to transfer the bond tokens puts them up for sale by indicating the transaction data, in this way the DVP Smart Contract blocks the corresponding bond tokens.

This first step generates a unique identifier of the transaction called UUID, which will be used by the Participant who wishes to acquire the tokens that the other Participant put up for sale and the DVP Smart Contract has locked. This second step causes the DVP Smart Contract to lock the corresponding cash tokens in the Commercial bank wallet associated with the buyer. When the cash tokens and bond tokens have been locked, the trade is settled atomically, settling both legs simultaneously.

The **roles** involved in this use case are:

Participants	Enter the transaction details and transfer the bond tokens
Commercial bank	Settling the Cash Leg

Bond Coupon Payment

This use case simulates the payment of the coupon to bondholders, i.e. cash tokens are transferred to Commercial banks that have wallets associated with Participants that hold bond tokens. It has been implemented that the coupon payment is made automatically or manually in order to experience live.

To make the payment, a call is made to the Smart Contract Securities Manager, which identifies the bondholders and the Smart Contract Wallets Link identifies the associated cash wallets. When the holders have been identified, the ERC-20 Smart Contract performs the transfer of wCBDC tokens to the corresponding wallets.

In this use case, the **roles** involved are:

CSD	Has the permissions of the Smart Contracts that correspond to the securities leg and manages the payment of the coupon
Commercial banks	Carry out cash transactions

Bond redemption

The redemption of the bond is simulated, i.e. when the date indicated in the bond characteristics arrives, the bond tokens are burned, and the corresponding wCBDC tokens are transferred to the Commercial banks. The date listed is called the “maturity date”, and the amount Commercial banks receive is the principal of the bond plus the last coupon payment.

The DVP Smart Contract locks the wCBDC tokens and the corresponding bond tokens, in this way an atomic settlement is achieved again and the bond tokens are transferred to a wallet in the possession of the CSD where they are deactivated.

The **roles** involved in this use case are:

CSD	Has the permissions of the Smart Contracts corresponding to the securities leg and owns the wallet to which the bond tokens are sent to proceed with their “burning”
Participants	Hold the bond tokens in their security wallets
Commercial banks	Receive wCBDC Token Transfer

Reporting

For this use case, several endpoints have been implemented that allow some queries to be made of data from the platform, whether it is the actors created, the bond issued or the Delivery vs Payment transactions initiated.

To obtain more information about this and to be able to delve into technical details of the platform, the transaction explorer is used, in which you can consult all the transactions made on the platform and their details (Smart Contracts involved, tokens transferred, time, block in which the transaction is recorded...)

In this use case, the Operator takes on great importance, as it is the only player on the platform that has complete visibility of the cash leg and the securities leg. In addition to accessing the block explorer to see the detail of all transactions, the Operator can filter the transactions made by each actor, showing the detail of each of the transactions.

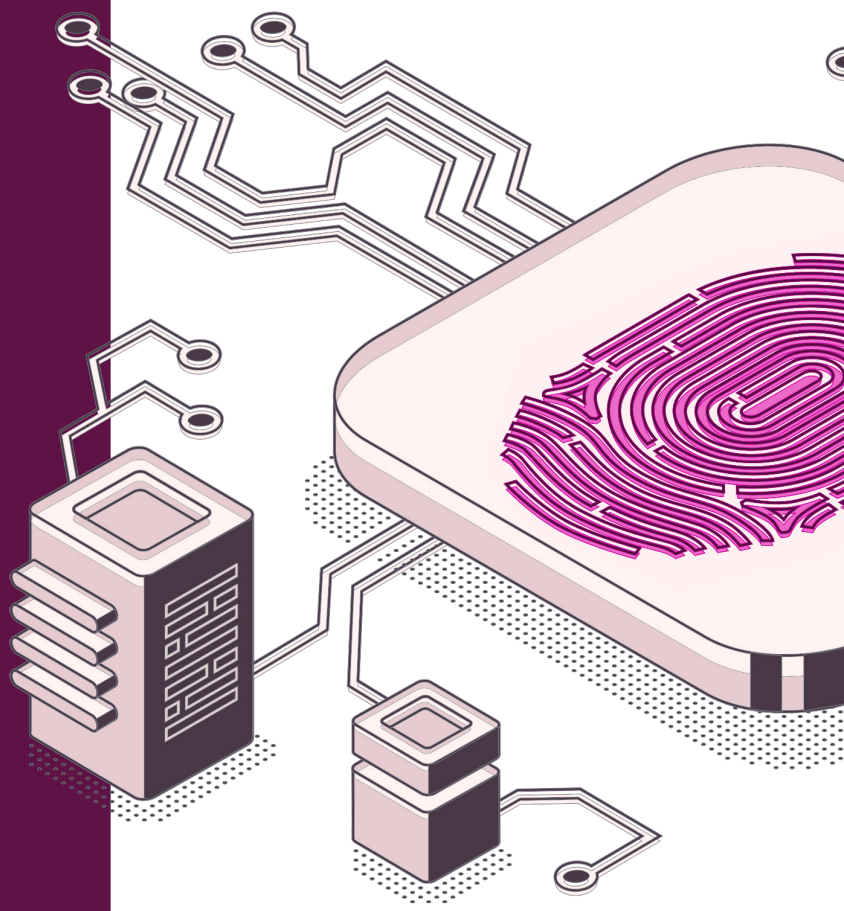
Evaluating the effectiveness of tokenization for the intended usage scenarios

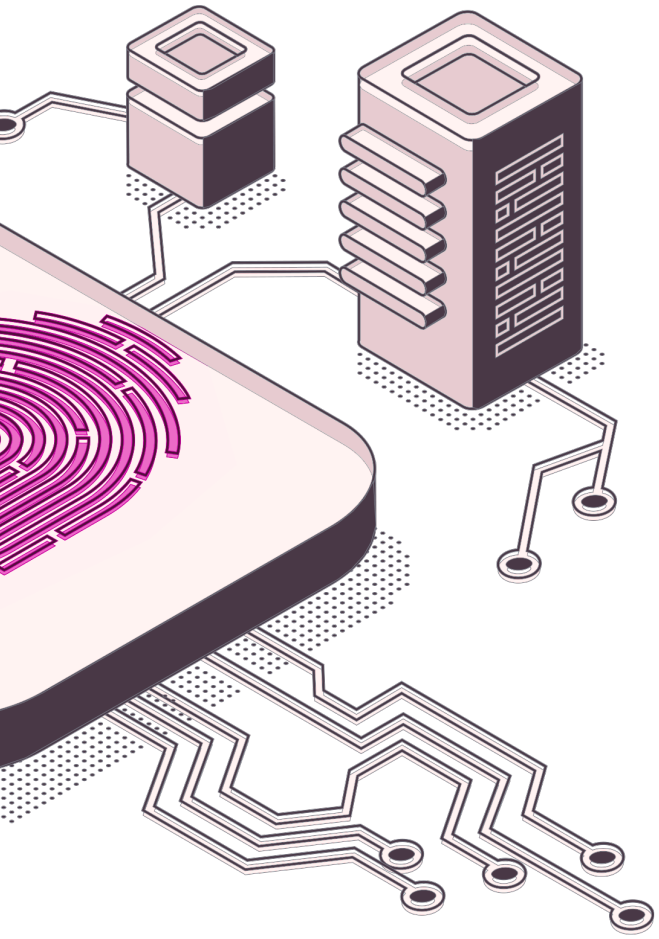
Areas for improvement in settlement as an infrastructure provider

Once the experiments were carried out, some areas of improvement have been identified with respect to traditional securities settlement processes and infrastructures such as Target2Securities. The experiments have been carried out on the system and have identified possible opportunities for improvement in terms of efficiency, safety and cost reduction.

The platform based on DLT technology could enable more efficient interoperability of intermediaries, optimizing their functions within the platform, which would lead to a reduction in costs and a streamlining of the settlement process.

The platform's actors can interact with the Smart Contracts deployed on the platform and thus save time and reduce risks, since these contracts allow the automation of processes, such as the registration of the Participants at the time of the subscription of the bond, and achieve an atomic settlement, ensuring that both the cash leg and the securities leg are settled at the same time.



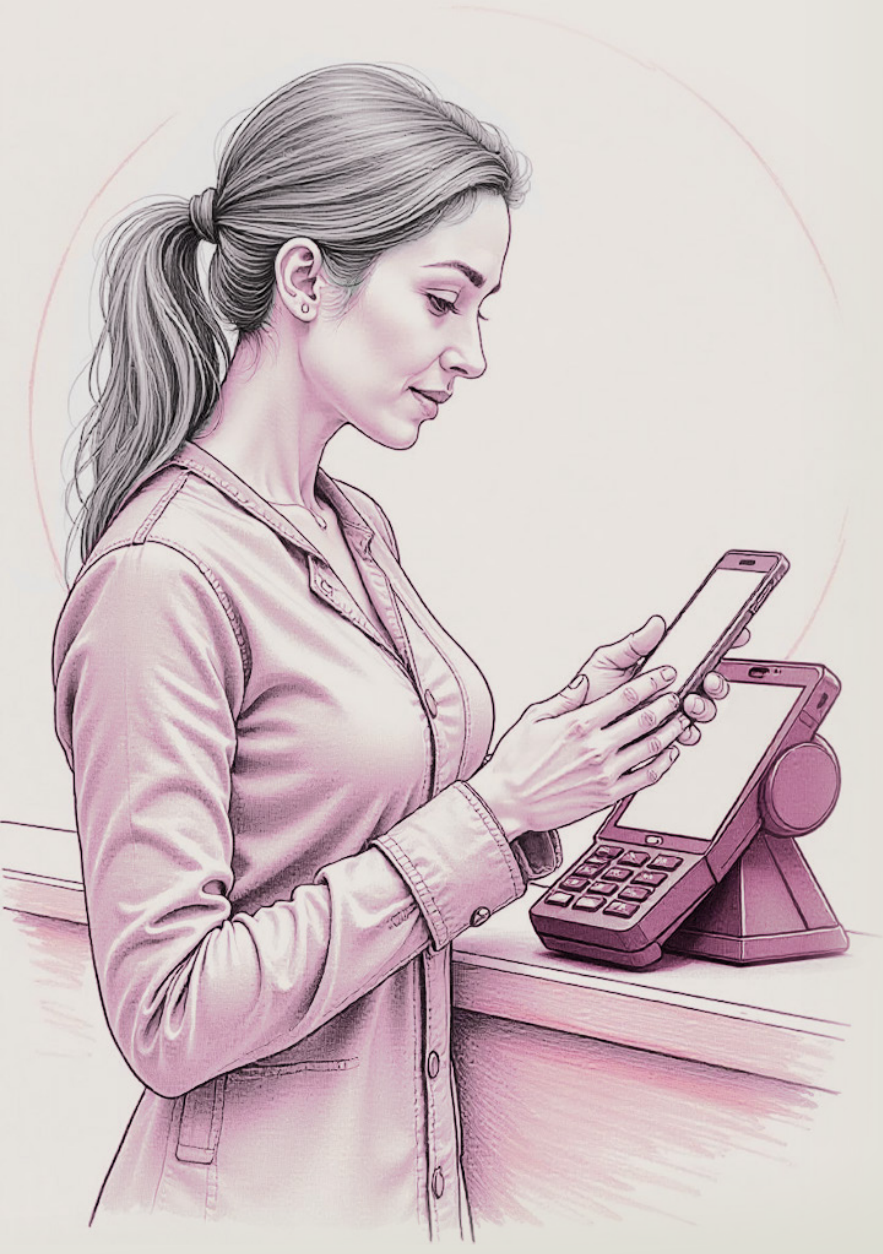


Commercial banks and Participants also take advantage of the minimization of counterparty risk, since thanks to the automation offered by Smart Contracts, this atomic settlement is achieved, that is, a process that involves the settlement of both parties simultaneously. With atomic settlement and Smart Contracts, settlement occurs in real-time, allowing immediate clearing of trades.

One of the most notable improvements of tokenization is in the efficiency with which bonds can be managed. This is largely due to the ability of Smart Contracts to automate a large part of the processes, since the digital representation of these bonds facilitates automation by converting them into digital tokens and allowing the programming of these tokens to execute predetermined actions when certain conditions are met, resulting in a reduction in times and costs associated with manual execution.

These enhancements, thanks to Smart Contracts and platform configuration, offer an advanced solution and a significant improvement in security, settlement times and risk reduction

Evaluate the potential business path associated with DLT technology in a new model of tokenized bond settlement and payment services



DLT technology has proven to have the potential to transform payment and securities settlement services by offering a more decentralized, secure, and efficient environment. In the context of securities settlement, this facilitates atomic settlement, minimizing counterparty risk and optimizing liquidity management thanks to the automation offered by Smart Contracts.

It is worth highlighting the improvement in transparency and trust of the parties thanks to the immutable and verifiable nature of DLT technology, which allows for real-time traceability of operations. In traditional models, actors rely on intermediaries to verify transactions. With this technology, processes can be automated and some can be eliminated, giving Participants the opportunity to have complete visibility of their operations and authorities to have more effective and less costly control, since with the introduction of Smart Contracts and a shared database, alternative business models could be contemplated.

If we focus on the scalability of the platform, transactions must be processed quickly to meet user expectations and business needs. While DLT technology offers a robust infrastructure, its distributed structure can introduce additional latencies compared to other systems. To do this, platform developers can adjust the consensus configuration and reduce the number of nodes to improve performance, always balancing between security and efficiency.

In the prototype, it was decided to use the minimum possible resources in order to save experimentation costs, specifically, experiments have been carried out with **two different configurations:**

Minimum configuration with fault tolerance

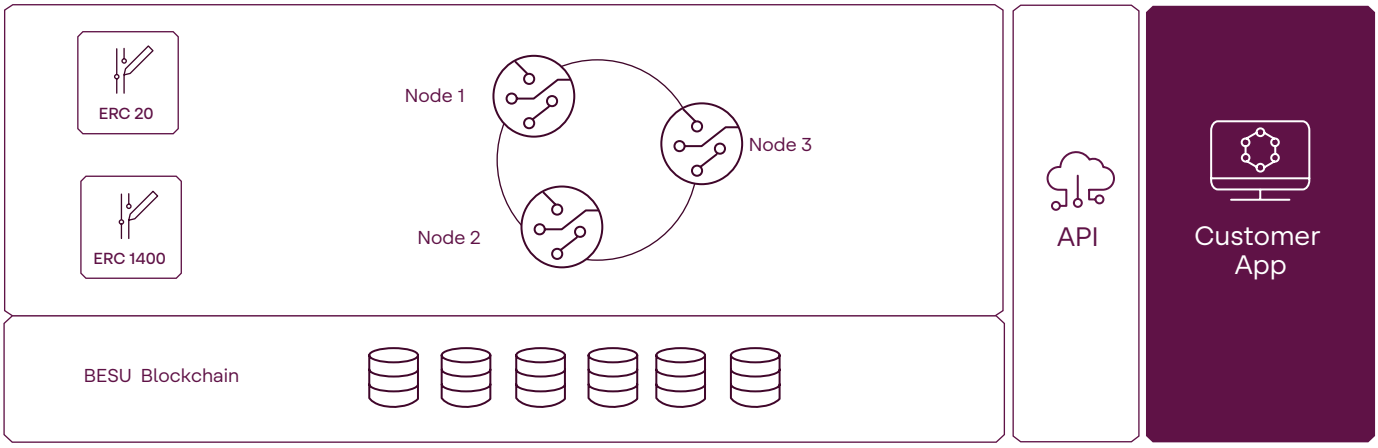
4 validator nodes

which with IBFT2 consensus, allows the failure or malicious operation of a node ensuring the correct execution of transactions.

Minimum consensus configuration

3 validator nodes

which is the minimum that IBFT2 allows to establish consensus



In these systems that process a large number of transactions, it is essential that regulatory and security standards are met. DLT offers a variety of security measures, such as data immutability or advanced encryption of wallets and Smart Contracts.
With an optimized design and solid control mechanisms, DLT technology, and specifically Blockchain technology, have the potential to facilitate a new model of settlement services, offering speed, security and transparency, increasing competitiveness and promoting innovation in financial markets globally.

04

Identification of the challenges and opportunities for the implementation of a wCBDC (wholesale Central Bank Digital Currency) and a tokenized bond

One of the challenges faced by the implementation of a Blockchain-based system capable of settling wCBDCs and tokenized bonds on a single platform is the way in which data is entered and processed.

In traditional systems we find the phenomenon “garbage-in, garbage-out”, which refers to the dependence on the quality of the data entered into the system. By integrating Smart Contracts into a DLT, mechanisms are established that can improve the quality of the information entered:

Process automation

Errors such as incorrect ISIN codes, wrong amounts, or mismatched settlement dates can lead to rejection of instructions or failure of the trade. The adoption of technologies such as DLT, where all Participants operate on a shared network, helps reduce these issues by ensuring greater synchronization.

Real-time validation

Smart Contracts run automated validation processes on the information entered before registering it in the DLT. If the data does not meet the pre-established conditions in the Smart Contract, the transaction or record is automatically rejected, preventing incorrect or incomplete information from being entered.

Traceability and immutable record

A key advantage of DLT technology is the immutability and traceability of the recorded information. Any data entered into the DLT network is permanently and auditably recorded.

In contrast to traditional systems, the single-platform DLT settlement model reduces, if not virtually eliminates, the risk of the emergence of the “garbage-in, garbage-out” phenomenon through a more simplified and secure architecture. The structure that allows wCBDC and tokenized bonds to be settled on the same platform has a single “Gateway”, which ensures that the information entered into the system complies with the rules established before being processed, minimizing the possibility of data errors.

MINSAIT | BANCO DE ESPAÑA Eurosistema

We connect
talent, technology
and business to generate
positive and sustainable
growth and impact.

Avda. de Bruselas, 35
28108 Alcobendas
Madrid, Spain
T +34 91 627 10 00
info@minsait.com