NATIONAL BANK OF KAZAKHSTAN

DIGITAL TENGE 2022
WHITE PAPER

Contents

Abbreviations

AML/CFT	(Anti-money laundering, Combating the financing of terrorism) A combination of tools and measures focused on countering money laundering and terrorist financing|
API	(Application programming interface) A description of the ways with the use of which one application/program can interact with another one
BIS	Bank for international settlements
BOC	bank of Canada
CAWI	Computer assisted web interviewing
CB	Central bank
CBDC	(Central bank digital currency) A digital form of a country's fiat currency
CI/CD	Continuous integration/Continuous delivery
C2C	(Customer-to-customer) Payments and money transfers between individuals
DB	Database
DevOps	(Development operations) A set of practices aimed to accelerate the systems development life cycle and provide continuous delivery with high software quality.
DeFi	(Decentralized finance) New financial technologies based on secure distributed ledgers
DLT	(Distributed ledger technology) An approach to store and share information within a non-fixed number of communication nodes and with the use of consensus achieveing algorithms to synchronize copies of data between participants
DSGE	(Dynamic stochastic general equilibrium) Macroeconomic modeling method used to analyze economic behavior at the micro level with respect to stochastic shocks
DT	Digital Tenge
EP	External participant
FI	Financial institution
GA	Government agencies
HTTP/2	(Hypertext Transfer Protocol version 2) An updated version of network protocol used by the Internet
ISO	International organization for standardization
IMF	International Monetary Fund
IS	Information security
KYC	(Know your customer или Know your client) Customer verification procedures
KPI	Key performance indicator
LCR	Liquidity coverage ratio
MVP	(Minimum viable product) A basic product with the minimum necessary characteristics created to experimentally test assumptions, to receive feedback from consumers and form hypotheses for further development
NBK	National Bank of the Republic of Kazakhstan
NFC	(Near-field communication) Short-range wireless transmission technology that enables data exchange between devices
OS	Operating system
PBOC	People bank of China
PFTDC	Payment and Financial Technologies Development Center
PoC	(Proof of concept) Project to develop a prototype platform (pilot platform) to test the viability of the concept of the Digital Tenge
PoS	(Point of sale) Electronic software and hardware device for accepting payment cards
PSP	Payment service provider
QA	Quality assurance

Abbreviations

Q&A	Questions and answers
QR-code	Quick response code
REST API	(Representational state transfer-based application programming interface) Architectural approach for creating application programming interfaces based on representation state transfer
RK	Republic of Kazakhstan
RTGS	(Real-time gross settlement) The system of continuous settlement of funds transfers in real time
R&D	(Research and development) Experimental study of new opportunities and services for the use of digital currencies
SHA-512	(Secure hash algorithm 512) Cryptographic algorithm based on unidirectional hash functions
SLA	(Service-level agreement) A contract between a service provider and its customers
SSH	(Secure shell) Application layer network protocol allowing remote control of the operating system
STB	Second-tier bank
TPS	Transactions per second
TLS	(Transport layer security) Cryptographic protocols for secure transmission of data between nodes on the Internet
UTXO	(Unspent transaction output) Cryptocurrency balances received by the user from each transaction in the blockchain
UI/UX	User's interface, User experience
USSD	(Unstructured supplementary service data) Service in GSM networks for sending short messages between the network subscriber and the service application
WB	World Bank

Summary

In accordance with the presidential instruction, the NBK implemented the "Digital Tenge" pilot project

In accordance with the presidential instruction, the NBK implemented the "Digital Tenge" pilot project in close cooperation with financial market participants, the expert community, and international financial organizations. The main milestones of the project are presented below.

The NBK's project delivery approach was guided by the principles of openness and transparency

The NBK's project delivery approach was guided by the principles of openness and transparency. Public discussions accompanied each stage of the project. The key architectural decisions covered all stakeholders' positions and best international practices. More than 100 meetings were held with market participants, international experts, and foreign regulators throughout the implementation of the project.

The technological potential of the DT enables to address new financial stability challenges

The key motivation for DT exploration was its potential for improving financial inclusion, promoting competition and innovation in the payments industry, thus increasing the competitiveness of Kazakhstan's financial sector in the global market. The new functionality of the DT platform also complements the existing payment systems. The technological potential of the DT enables to address new financial stability challenges including active development of the digital asset industry and decentralized finance.

The decision to implement the DT was made based on the study's results

The phased implementation over 3 years is recommended

The decision-making model for the DT issuance was developed to systematize the study. It included comprehensive risks and benefits assessment of the national digital currency issue. An Advisory Board consisting of independent international and Kazakhstani experts was formed to provide an objective analysis. A series of studies included a wide range of tools including technological pilot project and survey of the population. The decision to implement the DT was made based on the study's results. The phased implementation over 3 years combined with technological improvements, infrastructure preparation, and development of an operational model and regulatory framework is recommended. In this case, the DT system should be available for actual transactions from 2023 with a gradual expansion of its functionality and step-by-step introduction into the production scale by the end of 2025.

Digital Tenge public discussion report

APRIL 2021

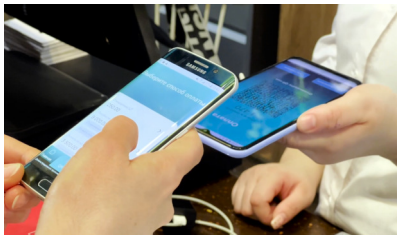
MAY 2021

DECEMBER 2021

Report on the results of the Digital Tenge pilot project (White Paper)

JULY 2022

Decision-making Framework



OCTOBER 2022

Pilot project with real consumers and merchants

THE DIGITAL TENGE WILL PROVIDE A WIDE RANGE OF UNIQUE OPPORTUNITIES FOR ALL CITIZENS

Cashless payment without Internet access

New financial services due to the programmability of tokens

Expanding the availability of financial services

Convenient settlements with the state without the threat to confidentiality

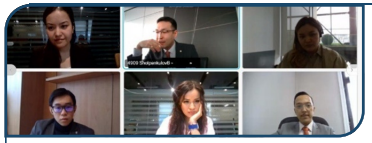
The Digital Tenge will be available through existing interfaces

Increased security and safety of funds with a high level of anonymity

Secure settlements in the field of digital assets and decentralized finance

Roundtable in the Senate of the Republic of Kazakhstan

Implementation of the national payment system. Digital tenge - expected results and development prospects



Set-up meeting with market participants

Participation in IMF and WB CBDC workshops

Community of technical experts

Tropical Africa Regional Conference on Digital Currencies and Crypto Assets

Digital Bridge 2022

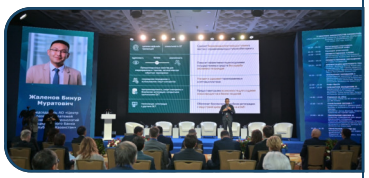
"CBDC: strategy and implementation goals" panel session

CordaCon 2022

More than 1,000 global financial services leaders, technologists and Corda enthusiasts from the CBDC to DeFi

Joint seminar of the National Bank of Poland and the Swiss National Bank

Digital finances



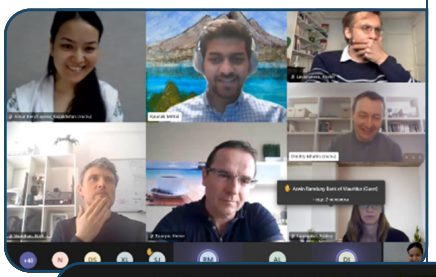
X Congress of Kazakhstan Financiers

The financial industry's role in the real sector development: challenges and opportunities

FEBRUARY — MARCH — APRIL — MAY — JUNE — AUGUST — SEPTEMBER — OCTOBER — NOVEMBER

Meeting with IMF and WB technical team

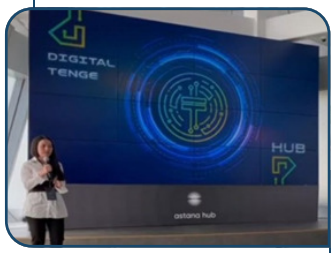
Presentation of technological aspects of the Digital Tenge project



Joint CBDC webinar of the NBK and the IMF

Q&A session with the expert community and opinion leaders

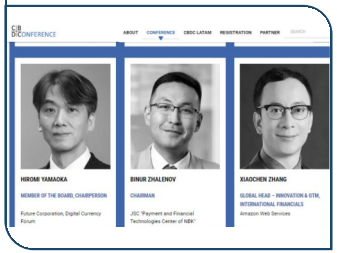
Implementation-related issues of the Digital Tenge project



Launch of the Digital Tenge Hub collaborative platform

Astana Finance Days

Digital Tenge and the global experience of the implementation of CBDC projects



International CBDC conference in Frankfurt

42 CB, 190 participants from 50 countries

General Council for Islamic Banks and Financial Institutions webinar

CBDC: How do they ensure a cashless society and the financial system stability?

CBDC Summit 2022 Washington

Masterclasses and meetings on CBDC in cooperation with the IMF and other CBs

PARTNERS

DISCUSSIONS WITH OTHER CBs

MEMORANDUMS

MEDIA COVERAGE

In 2022, there were

- 50 interviews and written commentaries
- 10 video interviews and live broadcasts on Kazakhstani TV channels and online platforms abroad
- 5 articles in specialized journals
- 1483 publications
- 2 mln views

Introduction

Digital Tenge (DT) is the third form of payment, which will be used along with cash and non-cash means of payment. The digital currency has the properties of existing forms of payment and provides new advantages for all market participants. Digital currency can be paid in the same way as cashless means - through Internet acquiring, mobile applications, POS terminals, QR codes, etc.

As in the case of cash, the DT is an obligation of the National Bank. Therefore, the DT payments do not carry the risks related to financial intermediaries. It is possible to pay using the DT without access to the Internet including also peer-to-peer (device-to-device) format.

In transfers and payments with the use of non-cash items, users do not feel the delayed settlement of interbank infrastructure transactions. But there are differences in the speed and settlement process in the DT. Payments in the DT system are settled instantly and finalized similarly to cash transactions. When tokens are transferred from the buyer's device to the seller's device, there is a transfer of monetary value similar to bills without financial intermediation.

The payment in the DT is more anonymous than in traditional non-cash instruments, and its confidentiality of payments is comparable to that of cash in some use cases. The DT allows the user to hide data from other participants in the system except for the wallet owner bank. When opening a wallet, the user gives access to his/her data to the bank to comply with AML/CFT rules. At the same time, it is possible to open wallets with a simplified identifier in accordance with the concept of risk-based AML/CFT supervision.

The unique advantages of the national digital currency include offline transaction chain capability and programmability. Compared to existing payment systems, the DT can conduct multiple transactions without access to the Internet while current card systems are limited to a single offline transaction, after which it is necessary to synchronize data in a centralized ledger and thus to have an Internet connection. The DT's programmability allows digital money to be endowed with special properties without jeopardizing the confidentiality of transactions: marking, targeting, etc. For example, it is possible to customize access to transaction data in the DT system (i.e., to hide individual transaction data) and to create smart contracts (i.e., to write the scenario's business logic for the process automation and intermediaries elimination).

The new advantages of the DT are created via hybrid technology that includes centralized elements of existing payment systems and decentralized elements of a distributed ledger.

While studying the DT's implementation, there were discussions on the issues of technological feasibility and reliability, the economic effect, relevant ecosystem development, the DT's operational model, and regulation of the DT's platform. All areas were studied step by step with respect to the views of all stakeholders and international best practices.

In 2021, the NBK launched a study on the possibility of implementing the DT in close cooperation with financial market participants, the expert community, and international partners. Throughout the study, the DT's properties (including the CBDC model parameters for Kazakhstan) were defined. Moreover, the technological viability of the DT concept based on the DLT was experimentally evaluated. There was also an initial model developed to assess the impact of the DT on the economy, financial stability, and monetary policy. In addition to this, possible approaches to regulation were studied.

In 2022, the NBK continued the study and also expanded the list of aspects to investigate:

1. **Technology** – technological feasibility of the DT's properties to achieve the implementation's goals and objectives
2. **Economics** – assessment of the potential benefits and risks from the introduction of the DT
3. **Ecosystem** – assessment of market readiness to use and implement DT
4. **Operational model** – analysis of possible options for system participants' interaction
5. **Regulation** – analysis of the DT-related legal regulation

To systematize the aspects above and thus assess the need for the implementation of the DT, a decision-making Framework was developed. The NBK designed its approach to assessing all benefits and risks from the launch of the DT that considers the goals and objectives of the development of the National Payment System of Kazakhstan.

Developed decision-making Framework considered all recommendations from leading international financial organizations (IMF & WEF) and subsequently identified all areas necessary for a comprehensive national digital currency implementation analysis.

Conducted analysis of the different countries' experience (including states that are currently implementing CBDC projects and those that have already implemented digital currencies) leads to the following conclusions.

The decision to conduct work on a digital currency depends on the initial goals and objectives set by the CB that depend on the type of digital currency, the country's economic development level, and the stage of implementation/study. Any CBDC-related decision-making process is influenced by the timing of the digital currencies investigation and implementation stages, as well as by the selection of the CB's priorities regarding digital currency (e.g., prioritizing the study of technology or economic aspects at the initial stage).

The most successful digital currency projects may have an initially fundamental goal that was achieved through experiments and pilot projects, and further attention was focused on other aspects (Sweden). Or, as in the cases of other projects, they were based on relatively simple KPIs (e.g., number of end-users), but these indicators were subsequently revised due to external factors (Eastern Caribbean countries).

There is no single decision-making framework for all cases due to different motivating factors, implementation timelines, approaches, and CB strategies.

The market participants' involvement is vital for making an informed decision. Therefore, the NBK ensured open communication with the market since the beginning of the project providing a platform for interaction between all stakeholders.

Decision-making Framework structure - document structure

The decision-making Framework consists of four main blocks that are covered in this report with all the results described.

1. The main parameters that determine the DT design
2. Definition of the DT design
3. Assessment of the DT design's viability
4. Conceptual analysis of the DT's operational and regulatory models

1

The main parameters that determine the design of the DT

1.1

Goals and objectives of the DT implementation

1.2

Criteria for the successfull DT implemetation with respect to local Kazakhstani principles

1.3

International principles of the CBDC implementation

2

DT design

3

Viability assessment

Cost-benefit analysis

Technology

Economics

Ecosystem

4

Operational model and regulation

NBK

Advisory Board

Comprehensive evlaution of results

Recommendation

YES?

Roadmap

Cost-benefit analysis

3 Viability assessment

Technology

Economics

Ecosystem

Decision-making criteria

01 Technological advantages/effects

02 Technological risks and cyber risks

03 Economic effects

04 Economic risks

05 Market and consumer readiness

4 Operational model and regulation

06 Regulatory model

07 Costs and benefits of the operational model

Comprehensive evaluation of results

NBK

Advisory Board

Goals and objectives of the DT implementation

The first chapter of this paper presents **the goals and objectives of the DT implementation**. All areas of the study are systematized into five blocks:

1. **Technology**
2. **Economics**
3. **Ecosytem**
4. **Operational model**
5. **Regulation**

The DT design is formed in the context of each area. For example, in the "Technology" section, the functional and non-functional requirements for the platform are defined with respect to the goals and objectives of the DT implementation. The DT's economic design is formed according to the principles of the DT implementation.

Each chapter of this paper covers specific research questions and hypotheses. The assessment approaches are developed with respect to these questions' specifics, and the study's main results and conclusions are also summarized for each direction.

	Goal	The DT's properties that can achieve the goals
1	Increased competition in the national financial market	The DT will provide opportunities for the market to create new products and business models via programmability, smart contracts, and secure integration with open DLT protocols
2	Increased proliferation of cashless payments	The DT will make cashless payments more accessible in places with limited Internet access via offline transaction chain capability
3	Ensuring continuous functioning of the National Payment System	The new functionality of the DT complements existing payment systems. The DT will be able to ensure the smooth functioning of the National Payment System even in case of shock scenarios
4	Increased efficiency of payments with the participation of the state	The DT will improve the efficiency of public spending without compromising the citizens' anonymity. The DT makes it possible to obtain a balance between targeting and payment anonymity via the targeted use of "marked" tokens with the possibility of automated "reverse marking" to ensure the anonymity of subsequent transactions
5	Increased financial market's competitiveness	Seamless integration of the DT with digital platforms inside the country enables the creation of new payment and financial products. For example, transaction settlement in "delivery versus payment" mode. The DT will also make cross-border and wholesale payments faster and cheaper by reducing intermediaries and using smart contracts. The DT can become a tool for regulating and monitoring transactions of traditional and decentralized finance through tokenization and integration with other DLT systems which is crucial in the context of global challenges.

In the future, implementing the DT will strengthen Kazakhstani financial market's readiness for new challenges.

Most of Kazakhstan's leading trading partners are actively implementing national digital currencies. Given the global financial infrastructure's increasing fragmentation trend, cross-border settlement in digital currencies may become a critical element of the trade and financial infrastructure. Thus, preparing the National Payment System for this scenario is vital.

Despite the so-called "crypto winter," the digital asset industry and financial tokenization continue to evolve. The significant jurisdictions' regulators are developing appropriate regulatory approaches, including prudential regulation of "stablecoins" backed by fiat currencies. These trends will lead to the increasing popularity of their use as a means of online payment. Uncontrolled distribution of digital assets among Kazakh consumers can cause "cryptoization" - the possible liquidity overflow from current accounts and deposits into stablecoins collateralized by global reserve currencies.

By using distributed registry technology, the DT can complement traditional financial infrastructure, which, on the one hand, provides consumer protection and macro-financial stability from the risks described above. On the other hand, it preserves the ability to use the innovative potential of digital assets.

Local and international principles of the implementation of the DT

In contrast to other CBs' approaches, the NBK focuses on the natural stimulation of market interest in the DT. Local implementation principles include:

1. Naturally developing market interest in the use of the DT in combination with the creation of new services and products with the DT without the use of administrative-command methods
2. Ensuring equal access to the DT system.
3. Customer-oriented approach focused on protecting the interests of consumers.

In addition, the business requirements for the DT consider the international principles for the CBDC implementation. The G7 principles are an extension of the basic BIS principles:

1) Fundamental principles of the implementation of CBDC

- *Existence of a legal and regulatory framework*
- *Data privacy*
- *Coexistence with existing payment systems*
- *Operational resilience and cybersecurity*
- *Illegal financial activities prevention*
- *International monetary and financial systems' stability*
- *Environmentally friendly use.*

2) Additional features of CBDC

- *Support for innovation in the digital economy*
- *Increasing financial inclusion*
- *Public sector payments*
- *Cross-border payments*
- *Support for the international cooperation development*

TECHNOLOGY

17-49
pp.

DT Design

The key technology-related goal of the project for 2022 is to study aspects of the implementation of DT and to test the technology platform's expanded functionality

The goal for the technological development in 2022 is to explore various aspects of the DT implementation. The extended functionalities' additional testing within the technology platform is based on the previously developed prototype. The decision on whether the DT should be implemented in the RK will be based on the implementation of the 2022 project.

Based on the goals and objectives of the project, as well as the international expertise, the key hypotheses were identified for testing via the Pilot Project.

The projec's results in White Paper 2021 describes the key parameters for the DT design

Within the current project, additional parameters for the design of DT have been determined

Additional design parameters of the DT were defined in the Project: Wallet Management Model, Approach to Anonymity, and A "Last Mile" Approach.

Key hypotheses to test in the pilot project

Hypothesis	Brief description
Ease of integration	Ability to easily connect external participants to the platform Integration with external participants' mobile applications Secure integration with open DLT protocols
Reduction of the number of participants	Ability to transfer value directly, without intermediaries Enablung DT tokens to be transfered directly from sender to receiver
Offline transactions	Technological feasibility for a chain of offline payments in case of problems related to the Internet connection in regions with insufficient internet coverage Allowing funds to be received offline and used in offline scenarios
Customizable anonymity	Ability to set user anonymity at the transaction level. For example, this function enables an individual to hide their data during the transfer process.
The balance of traceability and confidentiality	Enabling transactions traceability Ability to include AML/CFT compliance without the threat to consumer anonymity
Continuity of operation	No single point of failure Seamless operation 24/7 transaction availability
Programmability	Ability to limit target spending of funds by programmable tokens. For example, programmability enables the process of embedding information onto a type of token to track its use for special purposes.
Interoperability	Ability to ensure effective interaction with other payment systems
Transaction security	Transactions with the use of the DT system should be at least as good as transactions using non-cash funds in terms of information security and confidentiality

Correspondence between the objectives of implementing the DT in Kazakhstan and the project hypotheses

Decision-making model problem / Hypothesis	Increased competition in the financial market within the country	Increase in the penetration of non-cash payments	Ensuring the uninterrupted functioning of the National Payment System	Increasing the efficiency of payments with the participation of the state	Increasing the competitiveness of the financial market in relation to players from different sectors of the economy and other countries
Ease of integration	✓	✓	✓	✓	✓
Reduction of the number of participants	✓	✓	✓	✓	✓
Offline transactions	✓	✓	✓		✓
Customizable anonymity	✓	✓		✓	✓
Traceability	✓	✓		✓	✓
Continuity of operation	✓	✓		✓	✓
Programmability	✓	✓		✓	✓
Interoperability	✓	✓	✓	✓	✓
Transaction security	✓	✓	✓	✓	✓

✓ *Main effect*

✓ *Additional effect*

The functional and non-functional requirements were formulated based on the key hypotheses for implementation within the project.

Functional requirements

Functional requirements were included in the functionality of scenarios. The list of implemented scenarios contained the following ones:

- Basic MVP scenarios – basic scenarios for the DT life cycle (from issuance to circulation).
- MVP scenarios with advanced functionality - scenarios with the DT for special purposes, QR-based transfer scenario, reissuance, and monitoring.
- The R&D scenarios are scenarios for testing the innovative properties of the DT (e.g., offline transactions).

MVP and R&D Scenarios

BASELINE MVP SCENARIOS
Opening wallets of FIs/EPs or GAs
Opening wallets for individuals
Opening wallets for merchants
Issuance and distribution to FIs/EPs or GAs
Distribution to clients (standard DT)
C2C transfer (via mobile phone number)
Purchase with standard DT (online-mode)

MVP SCENARIOS WITH ADVANCED FUNCTIONALITY
Token marking
Distribution to clients (special DT)
Purchase with special DT (online-mode)
C2C transfer (via QR)
Reissuance (incl. technical redemption)
Monitoring

R&D SCENARIOS
Offline payments (with a chain of offline transactions)
External Participant's Scenario (BTS): fare payment
External Participant's Scenario (Eurasian Bank): opening a wallet, transfer, purchase

During the development of the platform in 2022, one of the key functional requirements was **vendor independence**, e.g., the independence from the supplier of the technology (including independence from the license and improvements on the vendor's side). To achieve the goal of ensuring technological independence in Kazakhstan, open-source software was used for the project.

Non-functional requirements

Based on the expected results from the DT platform software development (MVP and R&D), key hypotheses, and infrastructure characteristics, the following non-functional requirements were formulated. The requirements could be verified analytically or by conducting tests.

Requirements verified by conducting tests: assumptions that can be experimentally confirmed or refuted after passing the scenario as part of the pilot project or as part of the load testing.

Key hypotheses to test in the Pilot Project

Hypothesis	Requirement	Description
Continuity	Observability	The possibility of logging (tracking the status of the system and its components) and technical monitoring of the pilot platform infrastructure.
	Malfunctioning recovery	Mechanisms for backing up and restoring data from backups are provided for the production environment of the Pilot Platform (MVP). Manual database recovery from backups should be provided.
	Availability	The pilot platform's (MVP) availability should be no less than 95% during the pilot project, the maximum time of unavailability should be no more than 1 hour per day (in case of system updates).
Offline transactions	Channels	The architecture of the pilot platform (R&D) should provide the possibility of performing transactions through mobile devices without access or with limited access to the Internet. When access to the Internet is available, offline transactions should be synchronized and integrated into the overall transaction history.
Integration simplicity	Integration with external participants	Integration with external participants should be implemented using REST API methods, a common way to provide an API used in any programming language and supported by numerous libraries

List of requirements verified by conducting tests within the pilot project

Hypothesis	Requirement	Description
Interoperability	Compatibility with international QR-code standards	QR-code requirements development with the national standard of ST RK 3712-2021 [9] (requirements for the QR-code data for accepting payments) and international standard ISO18004 [3] (QR-code symbology specification) consideration
	Financial Messages Transmission's Compatibility with international standards	API specifications and Pilot Platform API development with potential ISO20022 payment standards applicability [2]
Technical requirements (not included in any of the hypotheses)	Throughput	Performance measurements obtained from loading tests during the pilot project
	Latency	Average transactions latency during the pilot project should not exceed 5 seconds Duration of purchase and transfer transactions (Corda transaction, API integration, and display in the banking front-end) should not exceed 15 seconds

Requirements verified analytically: assumptions that can be experimentally confirmed or refuted only at the stage of trial operation of the platform. Practical testing of these tasks was not within the pilot project's scope, so these requirements were verified analytically.

List of requirements verified analytically within the pilot project

Hypothesis	Requirement	Description
Continuity	Possibility of transfer to other infrastructure	The platform should be able to be transferred to another infrastructure without the need to make fundamental changes to the architecture and functionality of the platform.
	Scaling	The pilot platform (MVP) should include the ability to scale resources (vertical scalability) ensuring uninterrupted operation under high loads, as well as the possibility of further increasing the number of users and deploying across the National Payment System through horizontal scaling.

List of requirements verified analytically within the pilot project

Hypothesis	Requirement	Description
Ease of integration	Integration with open DLT protocols	The MVP architecture of the pilot platform can integrate with other platforms based on a distributed ledger. One of the ways to build integration can be the creation of technological bridges.

Information security requirements

Based on the expected results from the DT platform software development (MVP and R&D), along with the key hypotheses and infrastructure characteristics, the following information security requirements were formulated. The requirements can be verified by conducting tests.

Requirements verified by conducting tests: assumptions that can be experimentally confirmed or refuted after passing the scenario as part of the pilot project or as part of the load testing.

List of requirements verified by conducting tests within the Pilot Project

Hypothesis	Requirement	Description
Transaction security	Identification and authentication	The pilot platform (MVP) should provide identification and authentication of users and processes run on behalf of these users, as well as processes run on behalf of system accounts
	Role model	Access to reading and editing data of the pilot platform (MVP) should be limited by the implementation of the role-based access model
	Information security incident management	Information security incident management should be implemented during the pilot project (MVP). Monitoring and detection of incidents should be based on observations or technical instruments
	Information protection cryptographic mechanisms	Encryption algorithms should be applied using TLS and SSH protocols. Stored database access passwords should be protected using the SHA-512 encryption algorithm. Asymmetric cryptography algorithms should be used (elliptic curve cryptography): algorithms for signing and verifying a signature, creating one-time stealth addresses and one-time private keys to them, hiding amounts using the Pedersen commitment

Target Architecture of the DT Platform

A potential target functional architecture for a retail CBDC may have the following components:

- the core of the CBDC platform with business logic and platform integration and management tools
- integrated front-end solutions and service applications of platform participants
- connection to national-level systems
- interoperability with other DLT systems including within DeFi platforms.

The target platform is critical for the residents of the RK. It is necessary to implement and enhance protective measures that can save money, as well as ensure the financial stability of the RK.

In the target platform, it is necessary to:

- Provide independent maintenance, development, and scaling of the platform without third-party vendors or service providers
- Ensure the development of the platform, considering all the necessary information security technical means, principles, and practices;
- Implement network protection of the platform and communication channels;
- Provide access and rights management to the platform;
- Implement anti-virus information protection;
- Monitor, detect and respond to information security incidents;
- Manage privileged access as well as contractor access;
- Implement data leakage protection;
- Implement other information security measures, based on risks and best practices.

Approaching the choice of introducing the target technological solution

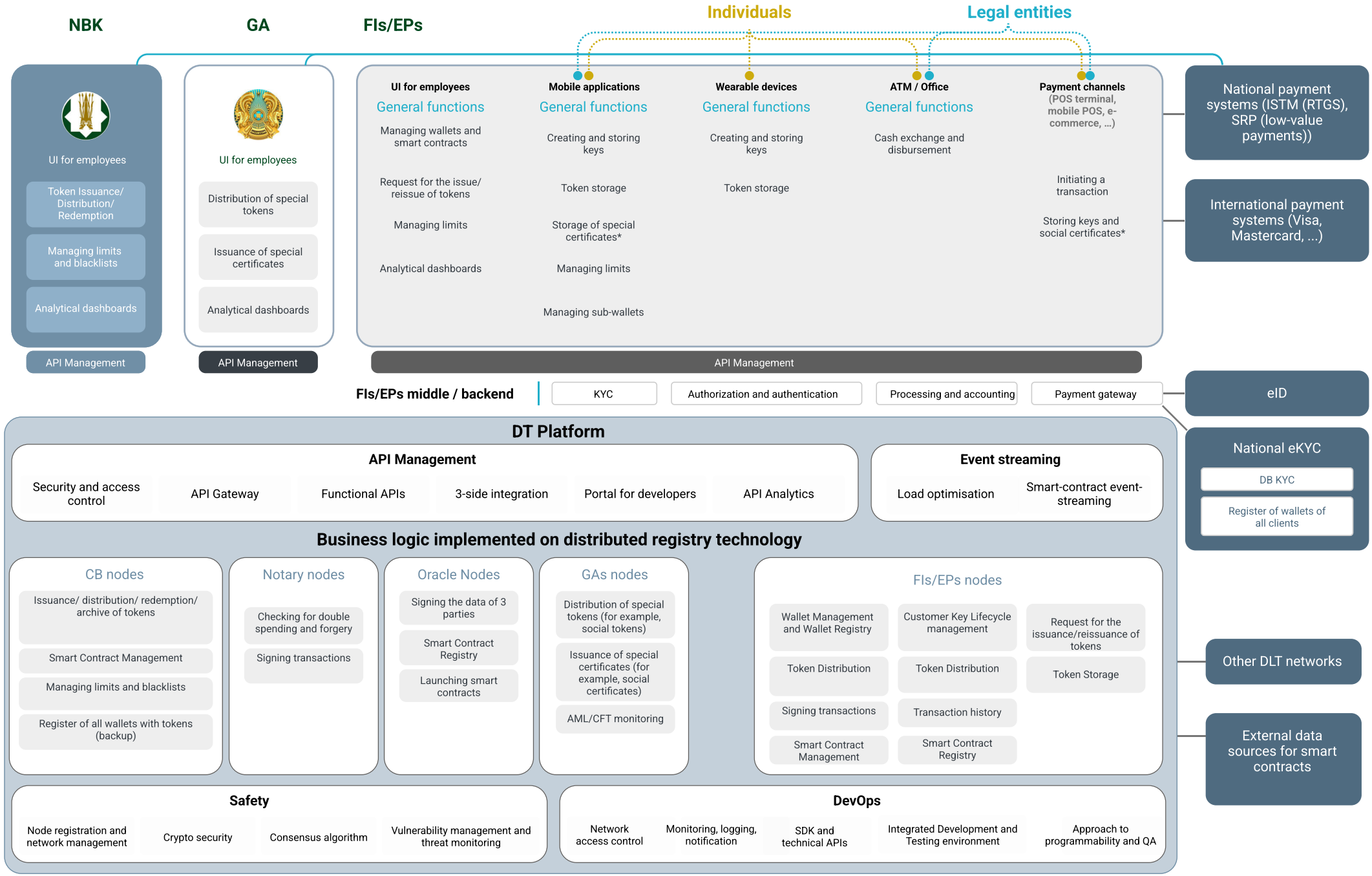
One of the key research areas for the subsequent stages of the project was the choice of the target technology for the distributed ledger. There were options for using a vendor-developed solution, as well as open-source software.

Based on the decision-making Framework and to continue the development of the PoC, the technological solution for the MVP and R&D was Corda R3 Community Edition platform. Corda R3 complied with the requirements formed for this stage of the project.

After testing and piloting in a closed environment, Corda was able to demonstrate acceptable performance results for the functioning of MVP and R&D scenarios. However, the acceptability of this platform for a production-grade solution should be tested in conditions close to real.

When choosing a target technology for the DT in the RK, the following three aspects were considered as crucial ones: vendor independence, uninterrupted operation of the system, and national technology sovereignty.

The availability of a flexible target architecture was also considered in the decision-making process. The flexible architecture will allow the implementation of various options for user scenarios in future stages (target scenarios will be determined at the next stage of the project).


NBK
GA
FIs/EPs
Individuals
Legal entities
UI for employees
Token Issuance/ Distribution/ Redemption
Managing limits and blacklists
Analytical dashboards
API Management
UI for employees
Distribution of special tokens
Issuance of special certificates
Analytical dashboards
API Management
UI for employees
General functions
Managing wallets and smart contracts
Request for the issue/ reissue of tokens
Managing limits
Analytical dashboards
Mobile applications
General functions
Creating and storing keys
Token storage
Storage of special certificates*
Managing limits
Managing sub-wallets
Wearable devices
General functions
Creating and storing keys
Token storage
ATM / Office
General functions
Cash exchange and disbursement
Payment channels
(POS terminal, mobile POS, e-commerce, ...)
Initiating a transaction
Storing keys and social certificates*
API Management
National payment systems (ISTM (RTGS), SRP (low-value payments))
International payment systems (Visa, Mastercard, ...)
FIs/EPs middle / backend
KYC
Authorization and authentication
Processing and accounting
Payment gateway
eID
National eKYC
DB KYC
Register of wallets of all clients
DT Platform
API Management
Security and access control
API Gateway
Functional APIs
3-side integration
Portal for developers
API Analytics
Event streaming
Load optimisation
Smart-contract event-streaming
Business logic implemented on distributed registry technology
CB nodes
Issuance/ distribution/ redemption/ archive of tokens
Smart Contract Management
Managing limits and blacklists
Register of all wallets with tokens (backup)
Notary nodes
Checking for double spending and forgery
Signing transactions
Oracle Nodes
Signing the data of 3 parties
Smart Contract Registry
Launching smart contracts
GAs nodes
Distribution of special tokens (for example, social tokens)
Issuance of special certificates (for example, social certificates)
AML/CFT monitoring
FIs/EPs nodes
Wallet Management and Wallet Registry
Customer Key Lifecycle management
Request for the issuance/reissuance of tokens
Token Distribution
Token Distribution
Token Storage
Signing transactions
Transaction history
Smart Contract Management
Smart Contract Registry
Other DLT networks
External data sources for smart contracts
Safety
Node registration and network management
Crypto security
Consensus algorithm
Vulnerability management and threat monitoring
DevOps
Network access control
Monitoring, logging, notification
SDK and technical APIs
Integrated Development and Testing environment
Approach to programmability and QA
* Only for sellers
CB systems
Participant systems
External systems
General functions
Authorization and authentication
Authorization of transactions
Crypto security
Tokens, viewing transaction history
API Management
Integration APIs
Backend-for-frontend

Key architectural decisions

White Paper published in 2021 described the key parameters for the DT design

Key DT design aspects

Design aspect	Description
Retail currency	The DT is a retail digital currency available to a wide range of users (individuals and legal entities).
Hybrid infrastructure	A combination of centralized and decentralized systems. Distributed ledger platform (DLT) was used which makes it possible to store, manage and keep records of digital currency and transactions with it. Also, the platform contains elements of the centralized system: • NBK ensures the connection of infrastructure participants (FIs/EPs, GA, etc.) to the platform • FIs/EPs ensure the connection of individuals and legal entities through an opening of digital wallets on the DT platform provided by NBK • No double-spending - it is impossible to use the same DT in different operations guaranteed by the NBK
Token-based model	Under the token-based model, the use of funds depends on the payee's ability to verify the valid payment object on the payment network
Two-tier architecture	• The NBK issues digital currency, monitors the security of the system, is responsible for the distributed ledger, and sets the criteria that must be met by the participants of the pilot platform. • Intermediaries (commercial banks, fintech organizations) interact with end-users: • Opening and servicing customer wallets, providing retail payments, KYC

When designing the DT architecture, a token-based approach was used. It implies that the CBDC exists in the form of tokens in a distributed ledger. As part of transactions, tokens are transferred from user to user. The transaction will be carried out successfully if the validity of the tokens used in the transaction is confirmed.

This approach made it possible to realize several additional advantages of the CBDC:

- Programmability at the token level;
- Conducting transactions offline;
- Customizable anonymity.

Additional design parameters of the DT were defined in the project: **Wallet Management Model, Approach to Anonymity, and A "Last Mile" Approach.**

Wallet Management Model

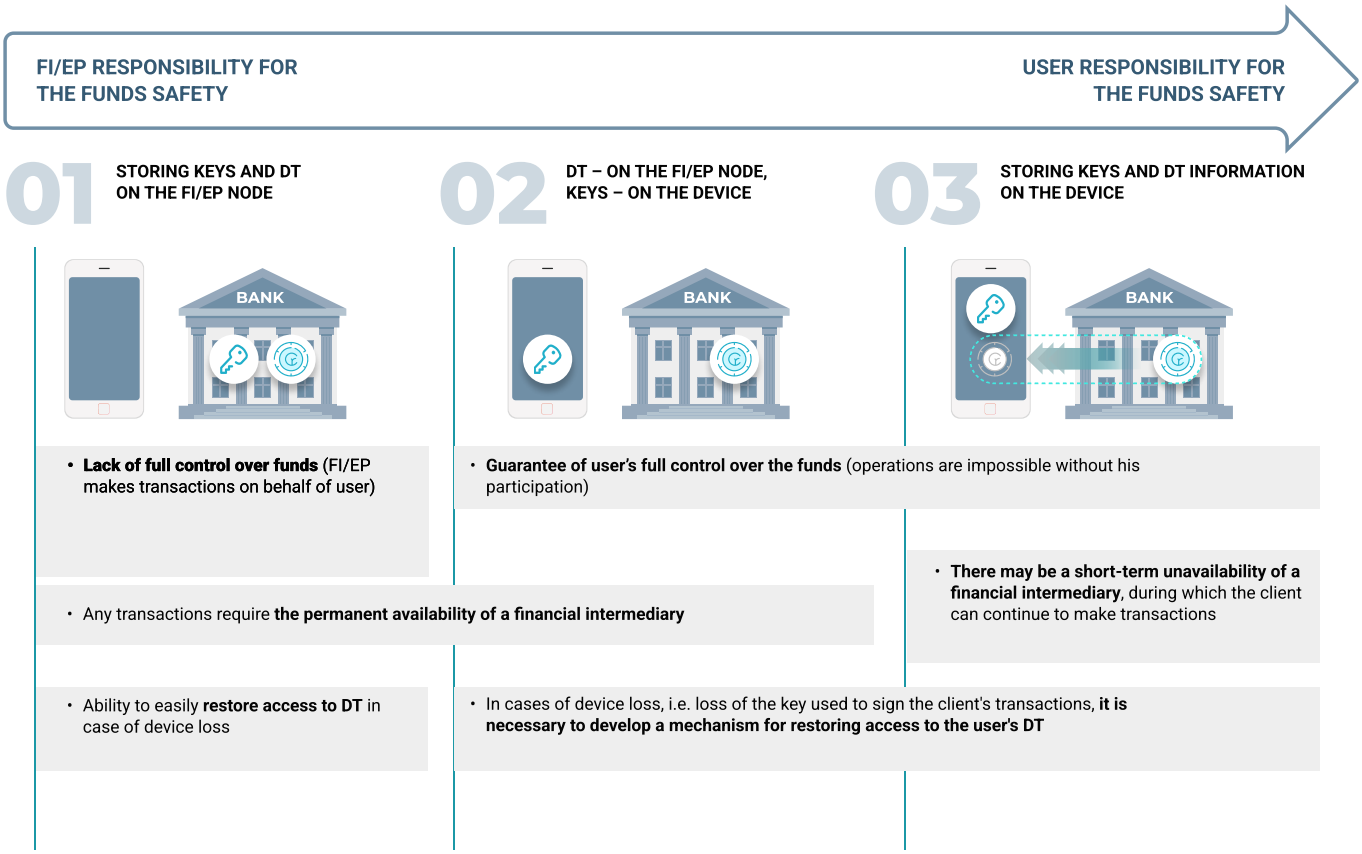
The platform implemented a two-tier model approach to wallet opening. FIs/EPs were responsible for opening client wallets. It was FIs/EPs' responsibility to comply with AML/CFT and KYC compliance. The NBK, on the contrary, was the operator of the pilot platform and was not involved in the process of opening wallets for individuals and merchants.

In the project a universal model was implemented: it was possible to open several wallets for a client in different banks (1 bank = 1 user wallet with different types of tokens).

The advantages of the chosen model included:

- Increased competition: the same product can be obtained from different providers. Financial players have more opportunities to compete for customers based on product properties
- Freedom for the consumer: flexibility to manage their money through different wallets. The possibility of controlling all wallets in different FIs/EPs through a single window can be realized through fintech services based on Open banking
- Consumer protection: there is no strict dependence on a particular FI/EP. Different FIs/EPs can implement different key storage models. The customer has the option to choose their preferred FI/EP. The selected FI/EP will have its own individual key storage model. Thus, the level of responsibility differs depending on individuals' willingness to bear responsibility for the security of their funds

There are three key and DT storage models:



In the first model, both keys and the DT are stored on the FI/EP's node (there is no transmission of bank-signed DT information to the customer's device). The model allows the customer to transfer full responsibility for the security of the funds to the FI/EP. The transactions are signed by the FI/EP on behalf of the customer.

The second model suggests keys storage on the customer's device. DT information certified by a bank signature is not transmitted to the customer's device. This model does not allow to use of the customer's funds without the customer's permission. This model requires the constant availability of a financial intermediary for transactions.

The third model suggests keys storage on the customer's device as well as the DT information transmission to the customer's device. This transmission is authenticated with a bank signature. In R&D, this action is referred to as a deposit transaction. The DT-related information appears on the wallet of the customers.

Before transmitting into the customer's device, the information is first signed by the FI/EP. When the customer transacts offline, the deposit information is transferred with a bank signature. To ensure the validity of the deposit offline, the signature can be verified by any other participant in the transaction.

Thus, the third model enables transacting offline, including cases when FI/EP are unavailable.

One of the important objectives of the R&D stream was to test the feasibility of a chain of offline transactions. Thus, Model 3 was used for offline transactions

In R&D a hybrid model was tested. The different ways of storing keys and tokens were used for online and offline wallets were explored:

Online wallet — 02

wallet with online mode support only

Implemented in R&D and by two external participants in MVP

Online wallet — 01

wallet with online mode support only

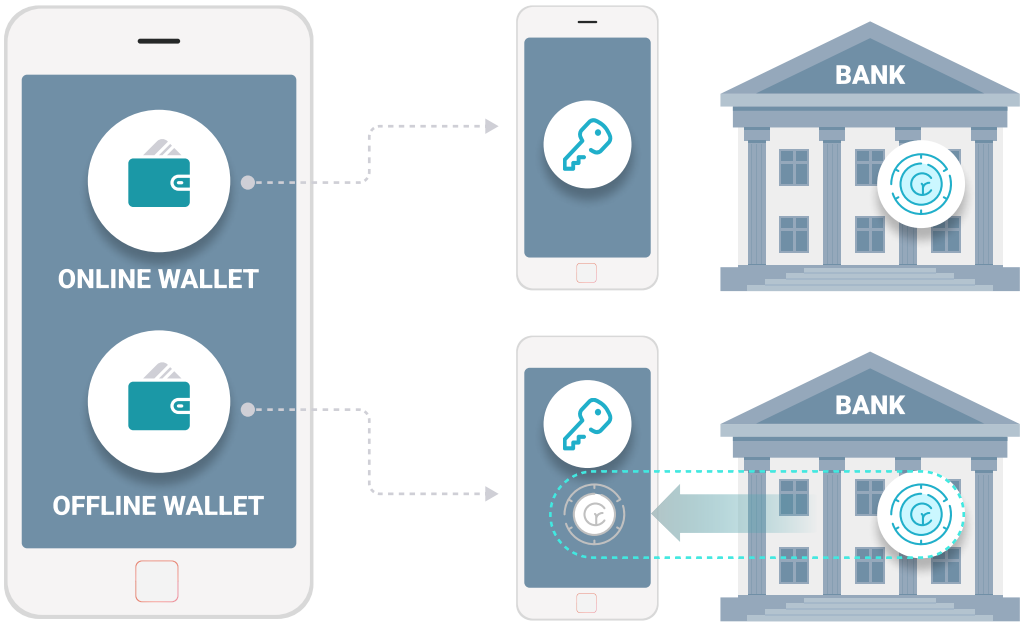
Implemented by one external participant

HYBRID MODEL:

ONLINE – DT IS ON THE FI/EP NODE

OFFLINE – DT-RELATED INFORMATION IS ON THE USER'S DEVICE

KEYS – ALWAYS ON THE USER'S DEVICE



— 02

— 03

The model in R&D created a pair of wallets: one wallet with only online mode available ("online wallet", Model 2) and a second wallet with offline transaction capability ("offline wallet" or "local wallet", Model 3). The **advantage** of the chosen hybrid model was the fact that it guarantees t**he user's sole control over the funds** (no transactions are possible without their involvement) and that transactions can be made offline.

Approach to anonymity

The 2022 project implemented fully identified wallets: the FI/EP knew the transactions of its clients.

A customizable anonymity logic was implemented - it allowed the customer to be anonymous to other participants. However, this was not the case for FI/EP where the customer's wallet was opened.

The solution architecture included a flexible wallet opening model. This model supported future decision-making on wallet types (including anonymity options) and future approaches to user KYC.

The model allowed the introduction of different wallet types depending on the level of user identification (e.g., anonymous within certain amount limits, partially identified, fully identified).

User anonymity

In MVP "customizable anonymity" functionality was implemented. The user had the option to choose to either disclose or not disclose their data to other users participating in the transaction. In the case where the sender wanted to remain anonymous, only the sender's node was be able to identify the sender.

The private view key allowed determining which primary public address one-time public stealth address corresponded to. This way, even if the customer wanted to remain anonymous, the bank could still meet the KYC and AML/CFT requirements.

Hiding information in a transaction

This model can also provide various options for the user to hide information in a transaction (e.g., hiding the transaction amount, token type, goods, and other parameters). In MVP, by default, the transaction amount was hidden from network participants (only the direct participants of the transaction know it).

Traceability

In addition, **different levels of traceability** were available depending on the DT type. A more detailed level of analytics was available for the special DT. For example, for the GA, the issuance of the special DT and the tracking of the DT's targeted use produced available analytics data on these DTs, i.e., the transparency of the use of the distributed funds increases.

A "last mile" approach

Since one of the criteria for the successful implementation of the DT was the n**atural development of market interest in the use of digital currency** (including the use of the DT in offline payments), an important decision during the DT development was to identify the carriers that could be used for offline transactions.

Solutions on offline wallet embedding in different carriers ("last mile" solutions) may be offered by different market providers (in cooperation with device manufacturers, OS, payment infrastructure vendors, and CBDC solutions providers).

The NBK (or another entity) is a centralized infrastructure operator of the DT. It is responsible for the selection, validation, and certification of such solutions to be used by market players (including certification from a security perspective, with a defined risk and incident management model for IS incidents).

Android and iOS were selected as the OS for the user device and the mobile PoS of the merchant.

Solution architecture

Architecture approach

An evolutionary approach was applied to the design of the DT platform architecture. As suggested by the decision-making Framework [8], **system flexibility, programming capability, and the implementation of offline payments** are identified as key technological functionalities. Based on the decision-making model and to continue the PoC development, the technological solution for the MVP and R&D was **Corda R3 Community Edition** platform based on the UTXO.

To achieve the DT platform **flexibility and its interoperability** with various external parties (GAs, FIs, fintech companies), a **multi-tier architecture approach** was used. It included the possibility of implementing the DT programmability at different levels (from the DT properties to the logic in the systems of external participants).

The DT platform's interoperability with other payment systems/financial mechanisms (exchanges, marketplaces, etc.) was supported due to the ISO20022 [2] standard consideration during the DT platform integration layer development.

QR-code was used in the transfer and purchase scenarios for the transmission of transaction details. To ensure the DT platform's interoperability in terms of the QR code work was carried out to determine the requirements for the QR-code, considering:

- existing national standard ST RK 3712-2021 (QR-code data composition requirements for payment acceptance) [9]
- international standard ISO18004 (specification of QR-code symbols) [3].

However, the true concern with the DT's interoperability is the weak accessible internet coverage across Kazakhstan. Poor network coverage poses a significant risk to the DT's penetration in all regions. Thus, the **implementation of offline payment chains** became the focus for the R&D phase, as producing an offline payment alternative may potentially address this problem.

Technological risks and platform stability were also important for the decision-making process. Distributed ledger technology with network access control for new participants and relational databases was selected for the project. Based on these technologies, a fully customized solution was developed and it was aimed to bring the following implementations: enabling necessary user scenarios, introducing an extension of the DT properties within the framework of programmability, and introducing configuration of AML/CFT monitoring on top of the DT platform.

Integration with external participants

An important criterion for the DT successful implementation is **to ensure equal access to the DT system**. During the project, the Digital Tenge Hub was launched, and market participants were invited to test the unique DT functionality. Scenarios were developed jointly with all participants who expressed interest in the project and presented ideas for further development of the DT.

The 2022 phase aimed to test the operation of external participants' **real mobile applications** integrated with the DT platform as well as to work closely with external participants to develop the platform (piloting scenarios, training on DLT development, and testing R&D hypotheses in the DT platform sandbox).

In MVP, integration with mobile applications developed by external parties (FIs, fintech companies) was implemented.

External participants were also involved in the connection of the developed mobile interfaces to the DT platform through an **integration layer API** (for user interaction and transaction initiation).

The first step towards building a dedicated API management platform for advanced management of access to the DT platform was **the implementation of access control to the platform at the application level via individual API keys**, as well as enabling employee access level to certain data.

To prepare for the pilot project, external participants were actively involved in training the pilot project's participants (merchants and individuals) and in organizing the user support process during the testing of the MVP.

The applications developed by external participants were used by the users during the DT platform piloting.

Within the R&D stream, a separate **"technology sandbox"** was created to conduct experiments. It was deployed as a separate environment provided by the PFTDC based on the codebase implemented in the MVP stream.

Hypotheses and research questions

The main goal of the 2022 pilot project was to test the DT's advanced functionality, conduct the DT piloting on real users, and experimental testing of the innovative DT properties.

Among the key issues of the technological solution are the following:

1. **Programming capabilities** – the DT's programmability implementation and testing with external participants, specifically, the ability to set restrictions on the use of the DT in the token structure to facilitate traceability of the intended use of the DT.

2. **Chains of offline transactions** - the technological feasibility of multiple transactions without the Internet connection between the sender and the receiver of the funds.

3. **Ease of integration** - the ability to easily connect external participants to the platform, the integration with external participants' mobile apps, and the ability for external participants to develop their scenarios in the technology sandbox.

4. **Customizable anonymity** – the possibility of transaction-level anonymity configuration (at the user's discretion)

5. **The DT as a possible means of payment** – testing the possibility of making payments and transfers using the DT.

6. **Performance optimization** including the implementation of the technical redemption functionality and replacing the old token with a long transaction chain with a new token with no history.

Assessment approach

In the technological aspects, the following approaches were set for 2022:

- Piloting lifecycle scenarios under near real-life conditions in a closed pilot environment with a limited number of participants
- Experimental study of advanced and innovative digital currency functionality and services

(such as the chain of offline transactions)

- Involvement of external participants in the project to jointly develop a vision for the DT implementation in Kazakhstan.

Description of MVP and R&D scenarios

№	Scenario	Confirmed hypotheses	Description
1	Opening wallets of FIs/ EPs or GA	Ease of integration	The initial creation of a digital wallet for the second-tier infrastructure participants (FIs/EPs or GA) to handle the DT.
2	Opening wallets for individuals	Ease of integration	The initial creation of digital wallets for individuals (FIs/ EPs clients). Wallets can only be opened in accredited (by first-tier-participant - the NBK) organizations.
3	Opening wallets for merchants	Ease of integration	The initial creation of digital wallets for merchants (FIs/ EPs clients). Wallets can only be opened in accredited (by a first-tier participant - the NBK) organizations.
4	Issuance and distribution to FIs/EPs or GAs	Transaction security	The initial DT tokens creation and the DT transfer from NBKs to second-tier infrastructure participants (FIs/ EPs, GA).
5	Distribution to clients (standard DT)	• Transaction security • Traceability	The process of transferring the DT from the FIs/EPs to the end-users, to the customer's digital wallet.
6	C2C transfer (via QR-code)	• Reduction of the number of participants • Customizable anonymity • Transaction security • Continuity of operation • Interoperability	The DT transfer from one individual to another at a short distance by transmitting the details through a QR-code with both the sender's and the receiver's devices connected to the Internet.
7	C2C transfer (via mobile phone number)	• Reduction of the number of participants • Customizable anonymity • Transaction security • Continuity of operation • Interoperability	The DT transfer from one individual to another individual via a mobile phone number with both the sender's and the receiver's devices connected to the Internet.

Description of MVP and R&D scenarios

№	Scenario	Confirmed hypotheses	Description
8	Purchase with standard DT (online mode)	• Reduction of the number of participants • Transaction security • Continuity of operation • Interoperability	Online purchase with the DT via merchants' and individuals' mobile apps (FIs/EPs clients) using a QR-code with both the sender's and the receiver's devices connected to the Internet.
9	Token marking	Programmability	Marking ("coloring") of the standard DT distributed from the NBK by a GA.
10	Distribution to clients (special DT)	• Reduction of the number of participants • Transaction security • Traceability	The process of transferring special tokens from a GA to end users, to the customer's digital wallet.
11	Purchase with special DT (online mode)	• Reduction of the number of participants • Programmability • Transaction security • Continuity of operation • Interoperability	Purchase with special DT (online-mode) via merchants' and individuals' mobile apps (FIs/EPs clients) using a QR-code, when both the sender's and the receiver's devices are connected to the Internet.
12	Reissuance (including technical redemption)	Continuity of operation	Token reissuance (technical redemption of tokens with history, issuance of new tokens without history) to reduce the performance load.
13	Monitoring	Traceability	Business analysis and monitoring of non-functional parameters.
14	Offline payments (with a chain of offline transactions)	• Offline transactions • Continuity of operation	A chain of the DT transfers using QR-code and NFC between digital wallets on different users' devices, with both the sender's and the receiver's devices not connected to the Internet.

№	Scenario	Confirmed hypotheses	Description
15	External Participant Scenario (BTS): fare payment	• Reduction of the number of participants • Programmability • Transaction security • Continuity of operation • Interoperability	Purchase with special DT (fare payment) via individuals' mobile apps using a QR-code, with an internet connection. There are restrictions on spending (time of use, amount of use per day, payment only in certain merchants).
16	External Participant Scenario (Eurasian Bank): opening a wallet, transfer, purchase	• Ease of integration • Reduction of the number of participants • Customizable anonymity • Transaction security • Continuity of operation • Interoperability	• Opening wallets for individuals: initial creation of digital wallets for individuals (FIs/EPs clients). • C2C transfer (via QR-code): The DT transfer from one individual to another by transmitting the details through a QR-code. • C2C transfer (via mobile phone number): The DT transfer from one individual to another individual via a mobile phone number. • Purchase with standard DT (online mode) • Purchase with special DT (online mode)

Functional characteristics

The scenario within the project is a functional characteristic of the platform which is a generalized description of the actions of one participant or the interaction of several participants in the pilot platform.

During the scenarios' development, the international and local principles of CBDC implementation were considered. The scenarios were designed in such a way that they:

1. Were customer-oriented (take the customers' interest into account as they go through the scenarios)

2. Ensured equal access to the DT system (applies both to external participants connected to the platform and individuals transacting using the DT)

3. Increased market interest in the use of digital currency (by adding innovative CBDC functionality such as offline payments, anonymity configuration, the DT programmability)

A user path for all participants (users of the DT platform) is presented below. The users walked through different scenarios of the DT lifecycle as well as additional innovation scenarios. Each of the steps in the user journey provided benefits and additional functionality for users (Appendix 1).

Piloting results

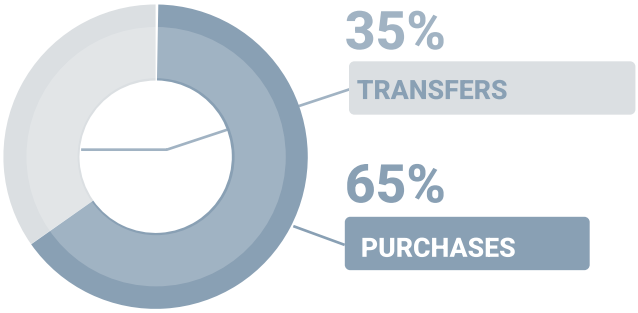
5 days

4 merchants

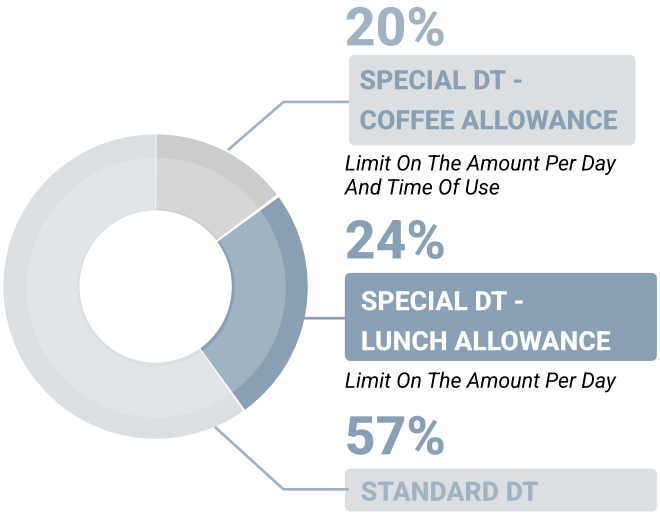
200 users

3 594 transactions

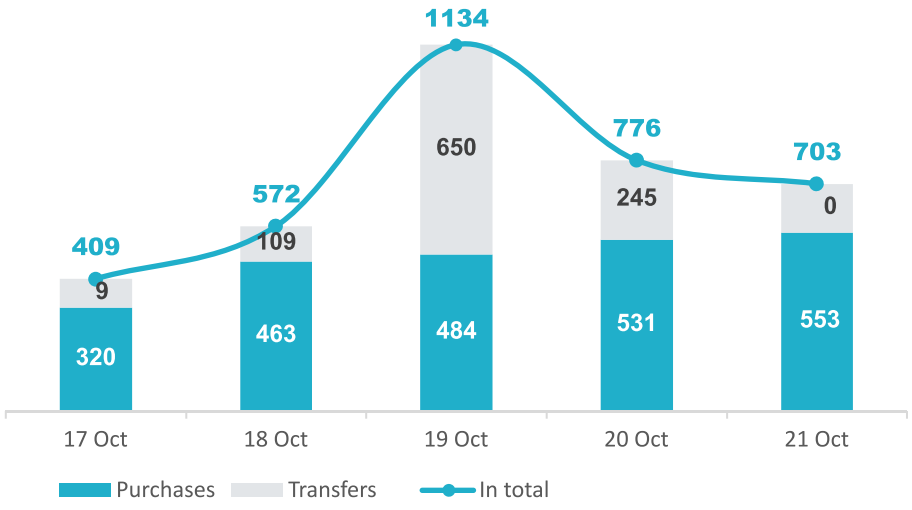
TRANSACTION TYPES



TRANSACTIONS BY TYPE OF DT



TRANSFERS – DYNAMICS



STRUCTURE OF TRANSFERS

40% BY PHONE NUMBER

60% BY QR

39% ANONYMOUS TRANSFERS

PILOT SURVEY RESULTS

96% STRESSED THE NECESSITY OF OFFLINE TRANSACTIONS

89% APPRECIATED THE IMPORTANCE OF THE DT PROGRAMMABILITY CONCEPT

77% NOTED THE HIGH SPEED TRANSACTIONS WITH THE DT

Results of offline payments research (with a chain of offline transactions)

The key goal of the offline scenario in R&D was to investigate the chain of offline transactions feasibility for each user. The development of this functionality will increase market interest in the use of digital currency, which corresponds to the criterion for a successful DT implementation.

Based on the study several results were identified:

- technical (protection against double-spending and anti-money laundering (AML) and countering the financing of terrorism (CFT), applicability and limitations of technology, device requirements, performance),
- functional (user-friendliness, the need for user limits)..

The following assumptions and limitations were defined for the chains of offline transactions study in R&D.

Assumptions and limitations of chain for offline transactions study in R&D

Assumptions and limitations	Explanation
The user could use offline mode on several devices, for this purpose a separate offline wallet is opened on each device. Within R&D, the condition 1 user = 1 device was applied. Offline and online wallets were within one bank.	Explicitly linking the offline wallet (and consequently the DT) to the customer's device, allowed covering one of the double-spending scenarios. Additional devices for the user would not meet the key research goal but would require additional labor costs
In R&D and demonstration mode, users were considered as trustworthy, they did not use fake tokens and did not commit illegal tampering with their devices. It was possible to verify the origin of the token offline from the moment the token is transferred to the offline wallet (deposit) based on the signature of the FI/EP (the bank acts as a guarantor for customers).	Ensuring absolute security in offline payments is a compicated and ambitious task which was beyond the scope of the current study. The target approach proposed to solve the security assumption based on last-mile solutions - software (crypto-protocols; secure code execution environment) and/or hardware (secure devices)
Offline transactions were carried out only with standard tokens.	Conducting a study with special tokens did not provide additional conclusions, as the main steps of such a transaction were the same as with standard tokens. One of the verification stages when paying with special tokens was performed at the mobile device level which was not included in the focus of the current research

Assumptions and limitations of chain for offline transactions study in R&D

Assumptions and limitations	Explanation
Transfer between users took place according **to the transfer scenario (transfer of requisites) and purchase.**	Description of the scenario, participants, and their functionality for an offline transaction in R&D.
Customers used Android devices with characteristics similar to MVP.	The Android research maintained continuity and the possibility of code reuse from the PoC stage. Research on two OSs (Android and iOS) would not significantly expand the study but would increase labor costs.

A list of open-ended questions was compiled for the R&D study:

- Possible mechanisms to reduce the risk of double-spending, money laundering, and terrorist financing
- Possible technologies for chains of offline transactions based on user-friendliness
- Possible length of the chains of offline transactions
- Technical requirements and limitations for users' devices for offline transactions
- Analysis of the need for functional limits applicable to an individual offline wallet
- Impact of offline transactions on node performance

The results of the research are presented in Appendix 1.

Exploring offline payments in other countries

Central banks of different countries are exploring offline payments. Below are examples of approaches to offline payments in different countries.

Examples of the approaches to offline-payments

Country	Approach
Kazakhstan	In 2022, a chain of offline transactions was tested with preliminary DT information transmission to the customer's device. This transmission was authenticated with a bank signature.
Russia [7]	To perform offline transactions, in addition to an online wallet, a second wallet in digital rubles was opened for the client on a mobile device. Replenishment of the offline wallet was carried out by the client by transferring digital rubles from the online wallet (in case of availability of an Internet connection).

Country	Approach
Sweden [5]	As part of the second phase of the E-krona development project, offline scenarios were tested in 2021: tokens and keys were stored locally on a mobile device, and NFC technology was used for data transfer. Synchronization of transactions required an Internet connection of one of the transaction participants.
China [4]	In collaboration with mobile phone manufacturers, the People's Bank of China was investigating offline smart card payments.
South Korea [6]	As part of the CBDC project, the Bank of Korea planned to launch offline tests on smartphones, smart watches, and Galaxy tablets from Samsung Electronics Co.

Results of token reissuance research (including technical redemption)

Reissuance may be defined as the old token (with a long chain of transactions) replacement with a new one (without any history). The scenario was designed to optimize performance: since transaction processing time increases as history increases, it is necessary to limit the maximum length of transaction history for the token to meet the maximum transaction duration requirements.

As part of the MVP stream, research on the token reissuance scenario was conducted. **The key objectives of this research are**:

- Optimization of platform performance and transaction time by reducing token history and verification time;
- Increasing the anonymity level of the DT platform by improving the traceability of broken transaction chains.

As part of the scenario, the "accumulation" value of the counter in the token's history was selected for the reissuance, based on the following factors:

- Optimization of client transaction duration;
- Possible routes of client transactions in the pilot;
- Optimization of the load on the system from transactions reissuance.

The research recorded the risks of reissuance and suggested ways to deal with them. There was no atomicity of reissuance (reissuance consisted of several transactions), the responsibility belonged to different participants (there was no single actor involved in each transaction), and no single contract (a transaction was valid if all contracts in it were executed without errors, but contracts were inside transactions and did not connect transactions). Technically, all four transactions cannot be combined into one.

The following arrangements were used t**o deal with the risks of the client losing money in the reissuance process**:

- Transaction sequence: first, new tokens were issued to the customer, and then the old tokens were sent to NBK
- All four reissuance transactions (issuance, distribution to individuals, transfer of token from customer to NBK, redemption) were linked using nested flow (each of four flow transactions was invoked within one large flow);
- Checks were implemented to prevent the FIs/EPs from spending the token issued as part of the reissuance beyond the reissuance;
- When submitting a request to NBK, the FIs/EPs marked the reissued token as being in the reissuance process. When the token was marked in this way, it could not be spent because the reissuance process had begun for the token.

Non-functional aspects

Performance

As a part of the pilot project, performance testing was conducted for pilot preparation. System check was also used to ensure the required level of performance during the pilot was with real users. The key areas of study during testing were:

- Transaction latency (seconds)
- Errors in transactions (percent)
- Infrastructure scaling effects
- Resources usage measurement (in terms of central processor units and random access memory)
- Potential areas for optimization

The developed DT platform can work on both Corda Community Edition and Corda Enterprise Edition. Load testing results showed that the platform covered the current pilot project's throughput requirements, but to achieve performance for a production level system, it is necessary to implement a few additional performance optimization solutions during development, regardless of Corda Community Edition or Corda Enterprise Edition being selected.

The greatest impact on the performance of the solution came from:

- standard Corda backup processes accounting for more than 75% of the data in processing each transaction;
- The presence/absence of multi-threaded transaction processing;
- Single-threaded processing when checking token transaction history.

Further recommendations for optimization are described in Appendix 1.

Pilot project performance results

During the pilot project, a comfortable performance level for users in making transactions was maintained due to the organizational measures (user transaction routes management within the pilot project, number of user transactions limitation), the tokens reissuance, and by the increasing system load resilience.

The pilot project results proved the technological feasibility of lifecycle scenarios and the possibility of applying the innovative properties of the DT. Performance optimization was not the focus of the pilot project. As part of the DT platform load testing, throughput and latency were measured with optimization methods and configuration settings being implemented. Time for full performance, stability testing and fine-tuning was not included at this stage.

The pilot project's results showed that platform performance on the same level as other payment systems would be one of the key challenges for the future. The DT platform at the next stage will require a deep study of performance issues and an allocation of a separate phase for research. It needs to explore the optimization and reach the following platform targets: increasing throughput, reducing transaction latency, solving the issue with transaction processing time increase with history increase (in addition to reissuing tokens), etc.

Observability and monitoring

The system provided **logging mechanisms** (**tracking the status of the system and its components**), as well as **technical monitoring of the MVP pilot platform infrastructure, non-functional indicators monitoring, and data for business statistics preparation.**

Interoperability

In the CBDC context, interoperability is a complex subject to consider due to many interactions and differences in data format with formats defined in existing standards. As part of the pilot project, **interoperability was tested in two aspects**: compatibility with international standards in terms of transferring financial messages and compatibility with international standards and national standards of Kazakhstan in terms of QR.

To check the compatibility of the DT platform with international standards in terms of transferring financial messages, API specifications and the DT Pilot Platform API was developed, considering the potential applicability of ISO20022 payment standards. Full compatibility was not achieved due to the fact that the existing standards do not support payment message formats for transactions with tokenized CBDC implemented with the use of cryptographic mechanisms involving the transfer of public addresses and signatures. Additionally, discrepancies in the transmitted parameters increase with functions for anonymity and programmability addition.

To check the compatibility of the DT platform with international standards and national standards of Kazakhstan in terms of QR-codes, the development of requirements for QR-code was done with the consideration of the existing national standard ST RK 3712-2021[9] (QR-code data requirements for accepting payments), as well as the international standard ISO18004 (QR-code specification) [3].

QR-code requirements development was done with a modification of the existing standard ST RK 3712-2021 [9] (requirements for QR-code data for accepting payments)

with an extension to the possibility of making transfers and payments in digital currency.

Thus, compatibility with international standards regarding the transmission of financial messages is currently not feasible due to the presence of unique features of the data transmitted within the CBDC platform. Full compatibility with international standards and national standards of Kazakhstan in terms of QR also requires modifications in existing standards.

Information security aspects

Information security areas are crucial for the DT platform and are described below. Within each aspect, a set of information security requirements was formed and the DT platform was assessed for compliance with these requirements.

Access control

The access control process was implemented with the consideration of personalizing all actions performed on behalf of users and processes launched on behalf of system accounts. To increase efficiency, account management used **the principle of grouping users** (for example, performing a certain list of work tasks), and conducted regular monitoring, review and, if necessary, accounts adjustment. Role model methods implementation in logical access differentiation enabled **the ability to optimally solve the problem of inventorying existing access rights for accounts** (such as temporary accounts that were necessary to perform tasks that require extended permissions). The password policies applied in the system were also fully compliant with the best information security practices.

Inventory and accounting

To ensure the correctness of procedures and processes for managing audit logs, the system time of the computer was synchronized via a network connection. This control ensured the consistent operation of the product and allowed it to effectively and timely investigate internal incidents while controlling any possible security breaches.

Audit log management

The event logs contained a sufficient dataset for potential security incidents investigation (information such as user IDs, session start and end timestamps, performed operations, and successful and rejected access attempts). The fact of confidential or redundant information presence was not recorded.

Information security incident management

The incident management process involved a formalized template for incident registration. The incident registration template was responsible to indicate the main parameters within the incident which helps determine which of the functional units within the DT platform are involved. For detected incidents, a three-level classification by criticality was introduced. The classification was based on the level of incident impacts on the performance. Also, the standard deadlines for notifying responsible persons and the investigation conduction were set.

Device and software configuration

The DT platform's environment architecture was implemented in a way that the production environment was separated from the test and development environment. It was designed to reduce the risk of making unauthorized changes to the production environment, reducing platform availability and/or data integrity loss.

Cryptographic information security mechanisms

To ensure transmitted information security in terms of confidentiality and integrity were practiced, encryption algorithms were based on TLS and SSH protocols. Stored database access passwords were protected using the SHA-512 encryption algorithm. Asymmetric cryptography algorithms (elliptic curve cryptography) were used: algorithms for signing and signature verification, one-time stealth addresses and one-time private keys creation, and hiding amounts using the Pedersen commitment.

Development security and vulnerability management

Only proven modules for encryption, logging, user identity management, and dependencies were used on the platform.

Since the target platform is critically important for the residents of RK, it is necessary to implement enhanced protection measures capable of preserving funds, as well as the financial stability of RK. For this purpose, in the target platform, it is necessary to:

- Ensure that the platform is developed considering all necessary technical means, principles, and practices in the field of InfoSec;
- Implement network security for the platform and communication channels;
- Ensure access and rights management for the platform;
- Implement anti-virus information protection;
- Monitor, detect and respond to InfoSec incidents;
- Ensure management of privileged access, as well as contractor access;
- Implement data leakage protection;
- Implement other InfoSec measures, based on risks and InfoSec best practices.

Evaluation findings

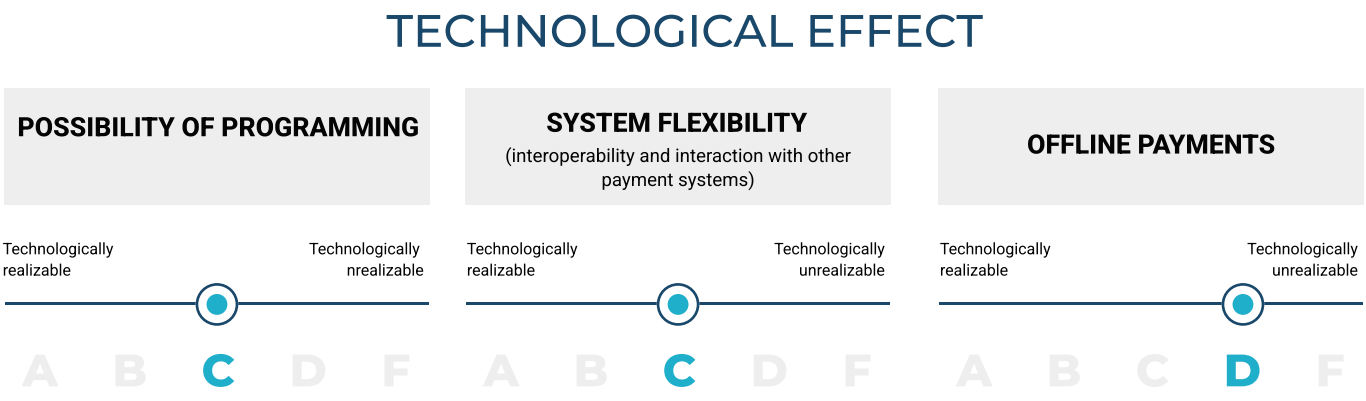
Assessment of the technological effect

Based on the pilot outcomes, the following results were achieved:

1. **Programming capabilities** – in MVP, the DT programmability was implemented and tested in the pilot project together with external participants, specifically, the ability to set limitations on the use of DT in the token structure to simplify the traceability of the target use of the DT (section 7.2.1). In the future, the functionality and programming capabilities of the DT will be expanded (for example, the implementation of smart contracts). According to the decision–making Framework, the technological feasibility of this functionality is currently posessing **the "C" grade** (this aspect is currently technologically feasible, but its implementation may require some additional analytical and research work and/or an insignificant number of resources).

2. **System flexibility** – the potential applicability of the ISO20022 payment standards [2] was assessed and integration with mobile applications developed by external participants (STB/fintech organizations) was implemented. Further implementation of the project will require integration with productive applications and systems (NBK, GA, FIs/EPs, merchants), integration with payment systems, and national services. According to the decision–making Framework, the technological feasibility of this functionality may be evaluated as having **the "C" grade** (this aspect is currently technologically feasible, but its implementation may require some additional analytical and research work and/or an insignificant number of resources).

3. Based on the conducted testing in R&D, **the technological feasibility of conducting transactions offline** (including the chain of offline transactions) was proved. To implement offline payments in a production-grade solution, it will be necessary to finalize the current solution (the use of several devices in offline mode and others). This means elaborating the following: a detailed of the "last mile" solutions, the regulatory issues, and the possibility of recovery. These aspect will require significant resources and research work (together with solution vendors). Based on the decision-making Framework, this category of technological effect may be considered as one with **the "D" grade** (this aspect is currently technologically feasible, but its implementation may require separate fundamental research and/or an average amount of resources).



The technological effect assessment grade for the DT implementation is "C" (this aspect is currently technologically feasible, but its implementation may require some additional analytical and research work and/or an insignificant number of resources).

Assessment of technological risks and cyber risks

During the implementation of the project, the following technological risks were identified:

1. Currently, **there are no technological solutions on the market that fully meet the requirements and properties of the DT**. The absence of a target technology for distributed ledgers and technological architecture places the implementation at risk. The limited understanding of the technology creates limitations such as not being able to fully assess the scope of work, and understand the timing, resources, and cost of the project.

2. **Choosing a vendor-supplied platform solution may reduce uncertainty in the development time but limits CBDC to out-of-the-box functionality**. Vendor platform solutions may create a strong dependence on a license, functionality on the vendor's side, and the support team's availability in ensuring the reliability of the solution. When choosing a target platform, it is necessary to consider technologies (and vendors supporting the development) that will ensure **the national technological sovereignty of Kazakhstan**.

3. **The risk of dependence on the technological maturity of external participants** – high-quality product implementation is possible in close cooperation with external participants. To implement the target platform, external participants will be required to invest significantly in the development of the solution (a certain level of technology stack and security of mobile applications, availability of competencies and infrastructure for integration with the DT platform, the possibility of functional development of the DT and compatibility with the main business of the external participant).

4. Due to the technological immaturity and a small number of production-grade implementations, **there is a risk that the platform will not provide performance comparable to existing national-level solutions**, for example, card systems. Currently, in the closed test environments, Corda and other technology platforms demonstrate are able to demonstrate acceptable performance results comparable to existing systems (for example, fast payment systems), but their acceptability for a production-grade solution should be tested in conditions closer to a more realistic environment.

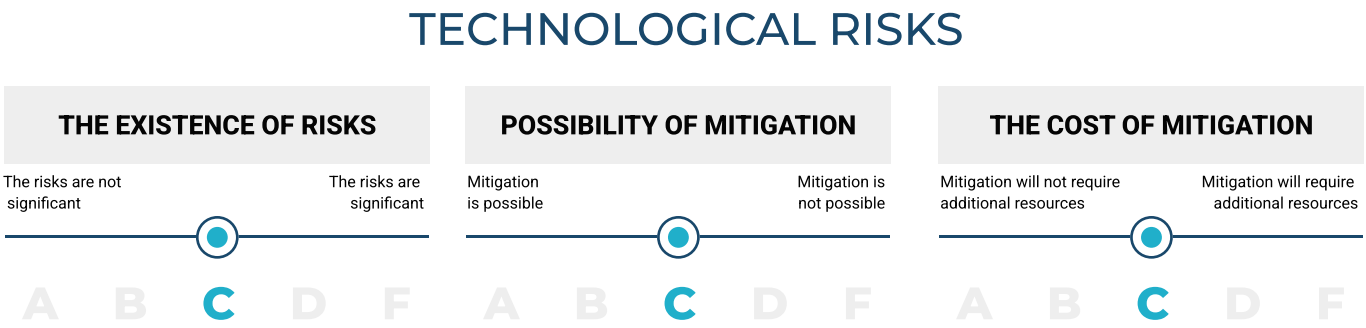
5. In general, **the security of the solution** is provided in two ways: built-in platform-level security and user-level security.

a. **Platform-level security**: currently, there is no single recommendation for the best implementation of platform-level security. The only few alternatives that exist as of now include algorithmic cryptocurrencies, hardware-based security, software-based security, or a combination of the two. Each option carries its risks and could only achieve a certain level of protection. The complexity of implementation and the "arms race" between attacks and protection remains to be a complex matter that needs to be addressed.
b. **User-level security** (security of "last mile" solutions) - user-level security should be guaranteed by the selected "last mile" solution (mobile app, smart cards, etc.). There are no existing decisions regarding "last mile" solutions. During the analytical study, potential solutions were identified, however, further interaction with vendors and partners for elaboration is required.

An A-to-F grading scale was used to assess technological risks according to the decision-making Framework by following criteria:

- The level of risk impact (where A - risks are not significant, F - implementation of the DT is associated with significant technological risks);
- Mitigation possibility (where A – mitigation is possible, F – mitigation is impossible);
- Mitigation cost (where A – mitigation will not require additional resources, F – mitigation will require significant additional resources).

Each of the mentioned risks was evaluated according to three criteria. Based on the risks listed above, it can be concluded that risks exist, but they can be mitigated. Thus, the technological risk assessment grade for the DT implementation is **«C»** (mitigating this approach's technological risks may require additional considerable research work and/or a small number of resources).



Cyber risks

During the development of a private information security threat model, it was that it would be crucial to identify security threat and their sources, prerequisites for implementation, and possible attack objects.

The consequences in the case of threats were determined by analyzing the possible negative effect when affecting three aspects of information security: confidentiality (C), integrity (I), and availability (A) of information processed by the platform. The assessment was carried out during the discussion of possible negative scenarios. The most significant ones were selected for each of the CIA directions.

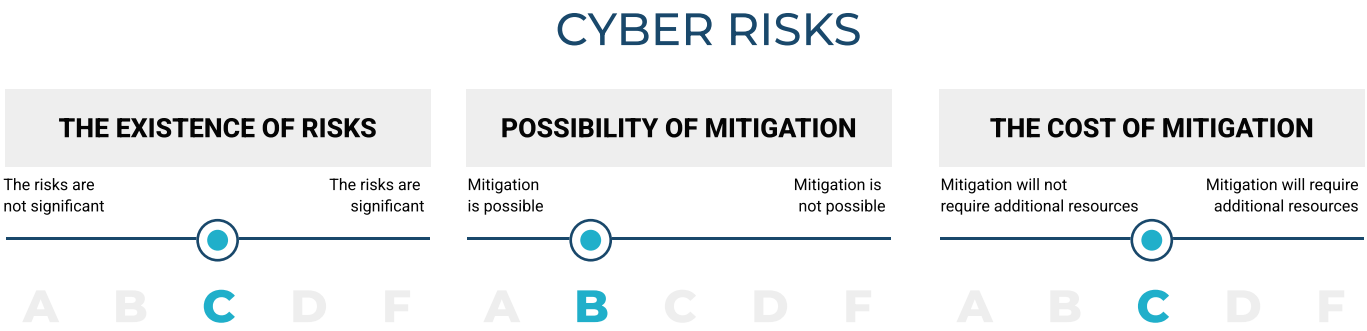
Based on the threat model analysis results, the most vulnerable objects of the platform were identified as the Node, the Node Database, and the network infrastructure.

A list of basic and advanced controls with a focus on proactive corporate asset management was recommended to prevent possible threats.

Based on the information protection analysis results, several mismatches with information security requirements were identified. Most of the mismatches related to the low level of information security processes formalization in the form of policies and other regulatory documents. It is important to understand that at the current stage of platform development (MVP) **it is not expected to provide user access to the data of the productive environment**.

Nevertheless, **a basic level of security was provided**. It can significantly **reduce the potential risk of InfoSec incidents and prevent damage to confidentiality, integrity, and the availability of the platform** including other related data. To increase the security level, it would be necessary to define a set of information security tools to plan their gradual implementation and future support.

According to the analysis results, the level of the platform protection corresponds to **the "C" grade** (mitigating this approach's technological risks may require additional considerable research work and/or a small number of resources).



The final assessment of technological risks and cyber risks is the value of "C" (mitigating this approach's technological risks may require additional considerable research work and/or a small number of resources).

Conclusion

The results of the project confirmed the technological feasibility of the requirements for DT

The results of the project confirmed the technological feasibility of the requirements imposed on the DT. Further work on the implementation of the CBDC in the RK will be the development of a production-grade solution.

Mitigation of technological risks may require a separate additional study

Such solution for the DT involves having baseline scenarios expansion to create competitive means of payments used by the entire population of the country. Therefore, it is worth highlighting several new functions as recommendations for production-grade solution development:

Infrastructure for the complex DT scenarios creation contains the following aspects:

The potential production-grade solution for the DT platform involves the expansion of basic scenarios to create a competitive means of payment used by the entire population of the country

- creation of a target API management platform to simplify integration and access control to the DT platform
- implementation of processes and tools for external participants' developments integration in the DT platform
- development of components for obtaining and validating external data at the DT platform level, including for the development of smart contracts
- Creating infrastructure for the development of complex scenarios with the use of the DT
- "last mile" solution choice with a focus on secure payments implementation at the country level
- optimizing the DT platform performance for high load
- the DT platform integration in the national and international financial landscape
- integration with basic universal services at the national level
- integration with national and international systems
- integration with other DLT systems.

ECONOMICS

51-58
pp.

DT design

The DT will complement existing payment systems and should not affect financial and macroeconomic stability

The economic design of the DT is based on the international principles of CBDC implementation. The DT will complement existing payment systems and should not affect financial and macroeconomic stability. In this regard, the design of the DT does not consider interest accrual, and the DT is primarily positioned as a payment instrument. With the participation of the NBK and payment service providers, the two-tiered digital payment system is preserved.

Limits and other financial regulation measures can mitigate the risk of liquidity flows from the banking sector to NBK obligations

In 2021, conducted assessment of the economic effects related to the DT implementation showed that its issuance would not increase the monetary base and money supply in the economy. There will be only changes in the money supply structure. In addition to this, the potential risk of liquidity flows from the banking sector to the NBK obligations can be mitigated by limits - permissible volumes of conversion of current accounts in the DT and other measures of financial regulation. According to recent BIS research, proposed measures to address the risks of diversion to CBDC are grouped into quantitative and price-based measures (Appendix 2).

As part of the decision making Framework in 2022, a quantitative analysis was conducted to assess two criteria: economic effects and risks.

Hypotheses and research questions

Economic effect

The implementation of the DT will bring a whole new range of digital opportunities and benefits to all citizens: consumers, financial institutions and government institutions.

Research questions:

1. What will be the demand for the DT?
2. Which of the attributes (characteristics) of the DT design - the cost of use, ease of use, security, anonymity, usefulness for budgeting, etc.- will affect demand?
3. To what extent will the DT affect the demand for cash and current account funds?

Economic risks

Along with the potential benefits, there are economic risks from the DT implementation, namely changes in macroeconomic parameters and the impact on financial stability.

Research questions:

1. How will macroeconomic variables change under different properties of the DT?
2. How would different rules for the DT implementation affect bank lending and borrowing activity in the economy?
3. What would be the impact of the DT on monetary policy?

Assessment approach

In economics, modeling tools are used to obtain quantitative answers built on empirical data. In the case of forecasting the demand for the DT, as well as for other CBDC, it is necessary to take into account the need for actual data on the use of payment instruments.

According to international practice, the assessement of the demand for the DT requires evaluating the behavior and attitudes of users towards existing payment instruments and the banking sector. For this purpose, in most cases, quantitative assessment methods based on Internet surveys of the population are used (Appendix 2).

Survey

Developed methodology for conducting the survey considered the DT design, socio-economic indicators of citizens of Kazakhstan, the specifics of the financial market and the characteristics of different types of products (cash, deposits, credit cards, etc.).

In contrast to other approaches, this survey included questions not only about current payment instruments in Kazakhstan but also about the characteristics that users would like to see in the DT. In addition, some questions that help to determine the willingness of Kazakhstani people to accept the DT were included. Namely, they defined characteristics that are most important to different segments of population. These questions are also direct indicators of the population's mood, level of trust, and demand for the DT. The survey questions about the DT were duplicated to understand how respondents' attitudes changed before and after receiving a brief explanation about the DT.

An online survey (CAWI) was conducted among 3,000 respondents. The number of respondents in all regions of Kazakhstan was quoted to ensure the representativeness of the sample, taking into account the demographic statistics, i.e. in proportion to the proportion of the adult population in the region to the total adult population. The survey data was used to build a micro-model to estimate the elasticities of substitution between the DT and its best alternatives: cash and current accounts (without interest payments).

Econometric model

Based on an econometric model, the potential demand for the DT was predicted. The relevant characteristics of the DT and households that affect the demand for the DT were identified (Appendix 2).

The constant elasticities of substitution between the DT and cash and these between the DT and current accounts were assessed. In other words, the model included the answer to the question “how easy or difficult is the interchangeability between cash, current accounts and the DT”. Higher elasticity led to the higher equivalence of them.

The success of the DT implementation depends on understanding which qualities of payment instruments are most important from the consumers' point of view, as well as the factors that increase the likelihood of using the DT. The model was constructed to examine consumers' attitudes toward the implementation of the DT. It evaluates the influence of various socio-demographic factors, knowledge of the DT, awareness of cryptocurrencies, importance of various DT characteristics, convenience of using cash and anonymity and trust in the servicing bank and the NBK.

One of the important features of the research methodology is the possibility to study the influence of various factors consisting of combinations of variables and other important factors due to the survey data including a wide range of questions [12, 17].

The probability of the DT being accepted by the citizens of Kazakhstan was calculated. On this basis, the impact of the DT on macroeconomic parameters, financial stability and the population's welfare was assessed.

2 DSGE models

An estimate of the constant elasticity of the DT substitution was integrated into two DSGE models.

These models took into account the unique structure of Kazakhstan's economy through equations and included the specific perception of households of the DT and other forms of money in Kazakhstan.

The uniqueness of utilized approach was based on the estimations of the obtained survey data's parameter, namely the elasticity of demand for the DT. Meanwhile, other institutons and CBs use indirect parameters due to the lack of survey data and the possibility of directly estimating the demand elasticity for the CBDC.

There a numerous other studies that fix the coefficient of elasticity of substitution on values not supported by empirical estimates. Also, macro- and micro-studies are usually conducted by different researchers, making it impossible to estimate this parameter in a micro-model (Appendix 2).

The elasticity of demand for the DT may be defined as an answer to the question "by how many percentages points does the ratio of the DT to money change for a one percentage point change in the relative costs of the DT and money". In this particular case, the costs include the costs of storage and commissions of use, while the price is the interest rate on the DT.

In general, there are only a limited number of papers analyzing the presence of CBDC in the DSGE model. The main conclusions are given in Appendix 2.

Survey

A survey of 3 000 consumers in all regions of Kazakhstan was conducted to collect data

Intermediate model

Next, a micro-econometric analysis was conducted based on the data in order to estimate the demand for the DT

2 DSGE models

The results were integrated into two DSGE models to assess the impact of the DT on macro-parameters, financial stability and the population's welfare of Kazakhstan

Study results

What will be the demand for the DT?

About 60% of respondents expressed their willingness to use the DT. The essential characteristics of the DT for the respondents are universal acceptance for payment, security (protection against fraud and theft) and lack of usage fees.

Men, compared to women, were more interested in using the DT, respondents from wealthier families were most inclined to try the new payment instrument, and respondents of older age were less interested in the DT. People over 50 years old are less willing to use the DT, but the difference with the category under 50 years old is insignificant - about 54% expressed a desire to use the DT.

The question about willingness to use the DT was asked twice in the questionnaire to see how greater awareness of the DT was reflected in the readiness to use it. It was repeated before and after reading an informational note describing the main characteristics of the DT.

Indeed, the respondents' interest in using the DT was more substantial with increased awareness of the topic.

Scenario analysis was used in assessing the demand for the DT. The desire to use it can vary depending on the different designs of the DT. People usually consider the existing practice when assessing the usefulness of the DT.

Which of the attributes (characteristics) of the DT design - the cost of use, ease of use, security, anonymity, usefulness for budgeting, etc.- will affect demand?

Five scenarios were analyzed: the DT with a basic design, the DT designed like cash, the DT designed like deposit, the DT designed like card and the DT designed like mobile app.

The following characteristics of the DT determined the design in the scenarios: convenience, cost, security, anonymity, widespread acceptance, convenience for personal finance (usefulness for budgeting) and bank bundling - an indicator of trust in banks and loyalty.

However, there is also another aspect of the design. It is important not only how the payment service provider designs it but also how it is perceived and used by the consumer. For example, it is possible to open a deposit but use it daily as current funds and perceive it as cash.

The baseline scenario assumes that the DT is more similar to cash: unrelated to banking services, interest-free, widely and ubiquitously used, and it has the same level of convenience, cost of use and security as cash. It is also assumed that the DT can achieve 70% cash anonymity and budgeting utility. Thus, in a basic scenario and design like cash, the demand for the DT is virtually the same.

In the baseline scenario, the projected demand for the DT for the month ranges from 9.7% to 24.4% of available funds, depending on how one perceives the DT: closer to cash or bank deposits.

If a consumer uses the DT as a payment instrument, the demand will be 9.6% for cash equivalents. If a person uses the DT in the form of a card, then the demand will be 38.4%. In the scenario of keeping funds in a bank as a deposit, the demand will be 48.1%.

DT design by service provider	The DT user's perception	
	perceives as cash	perceives as a deposit
Basic design	9,7%	24,4%
Cash-like design	9,6%	24,1%
Design as a deposit	23,8% perceives as cash	48,1% perceives as a bank card/app
Card-like design	24,5%	38,4%
Design as a mobile app	19,5%	26,5%

However, in the DT design similar to a mobile payment app the demand for the DT will drop to 26.5%. One of the main reasons is that people consider using mobile payments as an approach with higher utility. The transition from mobile payments to the DT may be more complicated than from cash or card payments to the DT.

Thus, the level of DT penetration largely depends on the design of the DT which should include the functions of mobile payment applications.

The level of DT penetration depends on understanding what qualities of payment instruments are most important from the consumers' point of view and what are the factors that increase the likelihood of using the DT.

The predicted probability of the population adopting the DT is 66.5%. The likelihood of using the DT is increased by the high calculation speed, convenience and operation through smartphones.

People with higher incomes have a high probability of accepting the DT, and the same is true for their employment status. Wage earners and the self-employed have a higher predicted possibility of adopting the DT than the unemployed. People who own businesses have a 58.3% probability of adopting the DT (the lowest among all employment groups). Businesses are less interested and more cautious in adopting DT.

Understanding business attitudes toward DT is another critical factor for successful implementation of the DT and it also should be explored in future research.

To what extent will the DT affect the demand for cash and current account funds?

The elasticity of substitution between cash and digital currency is 0.735. This value means that the average user is not completely ready to substitute cash for digital currency. For example, if the DT is less anonymous in relation to money and less convenient in personal finances, the DT will not be able to replace cash fully. At the same time, however, the coefficient demonstrates a high level of interchangeability.

The elasticity of substitution between current accounts and the DT is 0.609, so it is possible to state that users are less willing to substitute funds in current accounts for the DT than cash. The convenience of using funds in current accounts determines the extent to which non-cash funds flow to the DT. The present analysis shows that consumers do not perceive the DT as a 100% substitute for non-cash funds.

How will macroeconomic variables change under different properties of the DT?

Scenario analysis on macroeconomic stability

Various scenarios were analyzed:

1. The DT with zero interest rate
2. Issuing the DT as 10% of GDP
3. The DT with a fixed rate of 2%
4. The DT with variable rates, where the interest rate is determined through Taylor's rule

From the point of view of macroeconomic stability, the scenario with zero interest rate is the best one because it has the most negligible impact on output, inflation, the real exchange rate, and the budget deficit.

In the case of a zero interest rate on the DT, the volume of the DT would be between 5.7% and 6.2% of GDP in the long run. In other words, according to the economic notion of a long-term steady state of the economy, with a zero interest rate on the DT, the population would be willing to keep DT at between 5.7% and 6.2% of GDP.

In this case, there is no risk for financial institutions - with the outflow of current accounts of individuals from banks to the DT, the banking sector's profitability will not change because the DT is not an alternative for deposits and does not affect lending in the economy.

How would different rules for the DT introduction affect bank lending and borrowing activity in the economy?

The DSGE model with nominal and real rigidities was constructed to study the role of DT in financial stability in Kazakhstan. It included the banking sector, which was characterized by monopolistic competition. The model was based on [22] which studies the role of financial frictions and banking intermediation in business cycles.

Liquidity preferences augmented the model in the households' utility function which consists of cash and the DT. The model was then estimated using Bayesian methods and macroeconomic and financial data for Kazakhstan. After that, structural parameter measures were assessed. The economy was populated by a continuum of depositors, borrowers, and entrepreneurs. The following variables were chosen to determine financial stability: the interest spread of banks (difference between loan and deposit rates), the ratio of banks' equity to assets, the return on assets, and the return on equity of banks.

With a zero interest rate, the DT was used in the economy as a means of payment. The optimal demand for the DT by households was estimated between 5.7% and 6.2% of GDP. In this scenario, the introduction of the DT had an insignificant effect on the banks' profits and showed that the profits grew by 0.1% at a steady state (minor change). The implementation of the DT affected the structure of cash and current account balances of households, which are not a source of funding for loans. From this point of view, the DT has no impact on the process of profit formation and capital of banks (Appendix 2).

Moreover, further business sector surveys should be conducted next year to predict new revenues from introducing innovative scenarios with the DT.

What would be the impact of the DT on monetary policy?

The transmission mechanisms of financial shocks were practically unchanged due to the close interchangeability of cash and the DT. The impulse responses of key macroeconomic variables in the baseline scenario without DT and the scenarios with DT differed only in magnitude but not in the direction of the impulse responses.

The introduction of the DT allows the NBK to influence economic processes through the issuance and withdrawal of the DT from circulation. In this case, due to the imperfect complementarity (the constant elasticity is less than one and equals 0.735), cash and the DT moved synchronously so that liquidity in the economy reacted more strongly. When the base rate changed, the same trend was observed for the costs of holding assets in cash and the DT.

Therefore, a change in the base rate results in a change in the amount of money and the DT needed by households.

These are complementary types of instruments, so a change in one spurs a difference in the other instrument in the same direction, i.e., a feedback effect is created. In other words, when the NBK changed the base rate, the volume of liquidity changed more because of the complementarity of money and the DT. As a result, banks reacted by changing lending rates to a greater extent, which led to more pronounced changes in consumption and investment. This led to a more pronounced reaction of GDP and inflation in the economy.

The increased response of macroeconomic variables to the base rate means that the NBK may significantly impact the economy when the DT is implemented.

In addition, the economic effect - the change in the welfare of people in the economy with and without DT was assessed. When estimating the coefficient of substitution's constant elasticity, the convenience of using the DT (i.e., offline payment capability and programmability - both of them were further used in DSGE models) were taken into account. This means that all the characteristics of the DT measured by the survey data were also embedded in the estimated value of the substitution's elasticity coefficient between the DT and cash. The estimation showed a neutral effect, i.e., people's welfare does not change. Respondents in Kazakhstan consider the DT as money for transactions.

Evaluation findings

On average, the average user is willing to keep between 10 and 24% of funds in the DT per month

Analysis of the demand assessment results revealed that the average user is willing to keep between **10 and 24% of funds in the DT** on avereage per month. The probability of acceptance of the DT by the population is 67%. At the same time, the assessment of the economic effect - the change in people's welfare from the new benefits due to the DT implementation - showed a neutral effect. The welfare of people did not change in the scenario analysis with the introduction of the DT.

Scenario analysis regarding macroeconomic stability showed the optimal scenario for the introduction of the DT: without interest accrual

Scenario analysis regarding macroeconomic stability showed the optimal scenario for introducing the DT: demand should be between **5.7% and 6.2% of GDP in the long run** without interest charges.

Users are not ready to fully replace funds in current accounts on the DT, the interchangeability was only 0.609

The analysis of economic risk results demonstrated that the risks of the flow of current accounts' funds to the DT are controllable. Users are not ready to fully replace funds in current accounts with DT, and the interchangeability value was only 0.609.

The banking sector's profitability does not change, so there are no risks for financial stability

The implementation of the DT affects the structure of cash and funds on the current accounts of the population which are not a source of funding for loans. From this point of view, the DT has no impact on the profit formation process and banks' capital. In the optimal scenario, the banking sector's profitability does not change, so there are no financial stability risks.

The increased response of macroeconomic variables to the base rate means that a CB can have more influence on the economy with the DT being implemented.

The above conclusions indicate that the process of issuing and use of the DT as a third form of payment in Kazakhstan (along with cash and non-cash payment instruments) will not be a source of risks both for the stability of monetary policy and channels of its transmission mechanism, and for the stability of the financial system.

ECOSYSTEM

60-70
pp.

DT design

The potential benefits from the DT implementation can be realized only if the population widely accepts digital currency as a payment instrument

The potential benefits from the DT implementation can be realized only if the population widely accepts digital currency as a payment instrument. The example of Ecuador is solid evidence that the main reason for halted CBDC development was the low level of digital currency acceptance by the population and market participants [32]. From an ecosystem's point of view, the core value of the DT functionality is only achieved if the end users' benefit is identified. The implementation of the DT's payment infrastructure as a concept is viewed through the prism of three levels, and all of them have been under investigation since the beginning of the project.

1. Since 2021, many resources have been invested in the system's foundation development to ensure compliance with all basic requirements for the national payment system. This is the **base layer** – it is focused on providing equally accessible infrastructure for the DT transactions.
2. New opportunities are provided for all participants using the base layer, which may be called **add-ons**. They are additional services and innovative functionality determined by the DT's most essential properties, such as offline payment capability, programmability, anonymity, and targeting.
3. The main benefits for consumers – **value-added of new services and products** - are determined at the highest level of the DT infrastructure. The development of unique scenarios using the DT takes place during the formation of an ecosystem and the formulation of mutually beneficial rules for all participants.

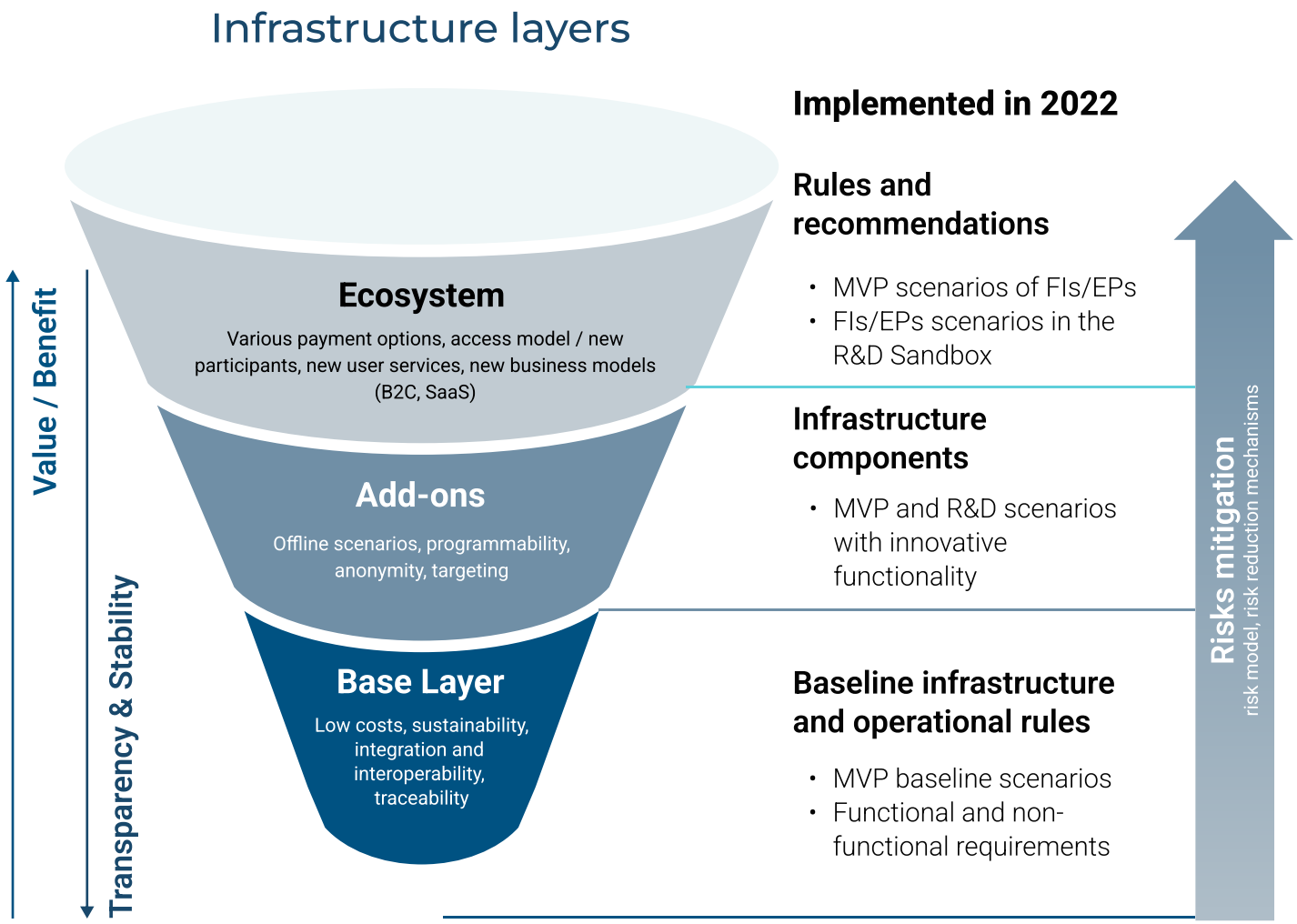
The main benefits for consumers – value-added of new services and products - are determined at the highest level of the DT infrastructure

The proper selection of initial business cases can be a crucial driver for creating an ecosystem for successful DT implementation in a staged manner

The two-tier model incentivizes the creation of innovative scenarios, and the target audience of such incentives are the market participants aware of consumers' problems. The proper selection of initial business cases can be a crucial driver for creating an ecosystem for successful DT implementation in a staged manner. Such scenarios should generate network effects, stimulate demand for the DT and create a market for PSPs. For this reason, the search for such business cases was one of the critical priorities, and the results of this search will be discussed below.

THE DT CANVAS:

The new DT infrastructure with shared overlay services with added value will contribute to the development of new services by the market ecosystem



Hypotheses and research questions

Evaluation of market and consumer readiness

It is necessary to complete a step-by-step work on the market participants' involvement to create all previously described system levels. During the research stage, the following questions were formulated to assess the market's readiness to accept the DT:

1. To what extent do market participants understand the DT concept?
2. To what extent are market participants interested in DT's further development?
3. What percentage of scenarios can be completed within the DT Hub?

The information below describes the tools used to find answers to these questions and the solutions themselves.

Assessment approach

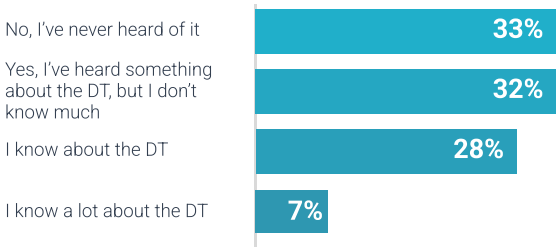
The main tools to assess the market and consumer readiness were

- market participants and consumers surveys on key topics related to the further development and use of the DT (also used in the "Economics" section)
- market participants' involvement in the joint development of scenarios within the pilot project
- interaction with market participants within the DT Hub

Study results

To what extent do market participants understand the DT concept?

The market participants and consumers survey provided information about the average level of immersion in issues related to the potential implementation of the DT. In particular, the survey data were used to determine the level of awareness of the Kazakhstani digital currency.



The chart above shows that just over a third of consumers in Kazakhstan possesses some DT-related knowledge (35%). Almost a third (32%) have a superficial understanding of the concept of the Kazakhstani digital currency, while 33% of respondents don't know anything about it. This level of awareness proves the need for further work to outreach to wider audiences because the level of understanding also affects the acceptance of the DT. This can be proved by the experiment that was previously described in the "Economics" section and included in the survey – the respondents were asked twice the question "If tomorrow the digital tenge was implemented in Kazahstan, would you use it?" in the middle and at the end of the survey.

The second time this question was asked after the respondent had been given brief information about the DT and its main characteristics. The data shows that the percentage of respondents willing to use the DT before the clarification was 60%. After providing a summary of the DT's properties, this value rose to 68% (see infographic below).

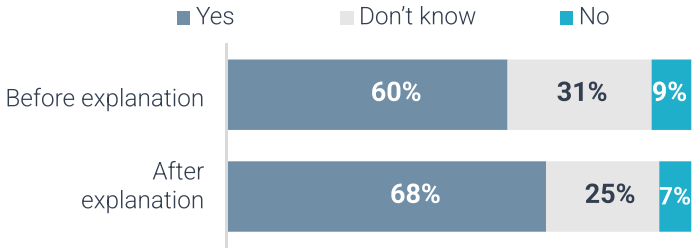
Due to the digital currency topic's novelty and the relatively large number of uninformed consumers, **resources should be allocated to clarify the DT's properties and popularize the DT as a payment instrument to increase the acceptance of the DT.**

It is also crucial to pay attention to the respondents' attitudes toward the properties of the DT. The chart below shows which digital currency's characteristics are the most important for consumers.

The acceptance of the DT by the population primarily depends on how the ability to pay with the DT is common. This aspect not only ranks first in the list of qualities that the DT should have (according to the respondents) but also reflects the main advantage of cash and one of the main obstacles to cashless payments. The second most important feature of the DT is security which is confirmed by technical failures being one of the main disadvantages of current cashless methods. In third place, respondents rated the possibility of paying without a commission, which should also be discussed later (see the "Operational model" section). The fourth place is occupied by the possibility of making payments without access to the Internet. This problem can be solved with the help of quasi-offline payment methods (via communication tools not intended for this, such as USSD codes or 2G protocols) and by implementing the functionality of conducting a chain of transactions offline. Finally, the DT's qualities, such as simplicity, convenience, and speed, are also important to consumers. As the survey results show, all three qualities can be attributed to cash and non-cash methods.

3000 respondents

"If tomorrow the digital tenge was implemented in Kazahstan, would you use it?"



Willingness to use the DT is higher among

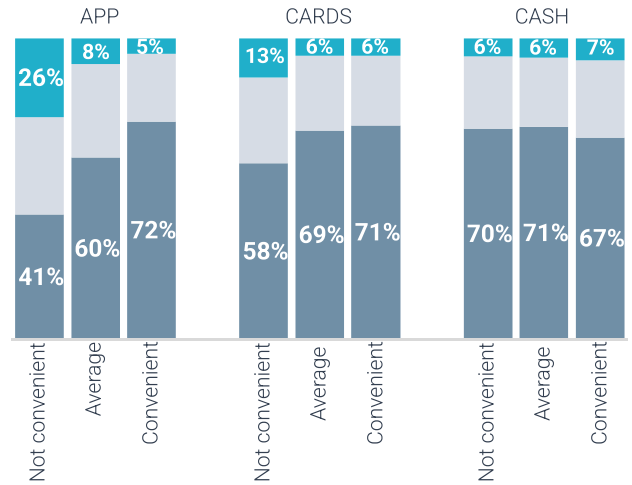
- persons with income over 500 thousand tenge per month - 79%
- Kazakh-speaking respondents - 71%
- students - 68%
- business owners - 68%
- self-employed persons - 65%
- men - 65%
- young people - 62%
- who use the bank app on a daily basis - 65%
- who use mobile payment services on a daily basis - 74%

The most vulnerable segments of society are not ready to use the DT

- persons with low income (up to 50,000 tenge per month) - 12%
- retirees - 15%
- disabled people - 13%
- people in the age of 51 and older - 11%
- people with a high school education or less - 11%

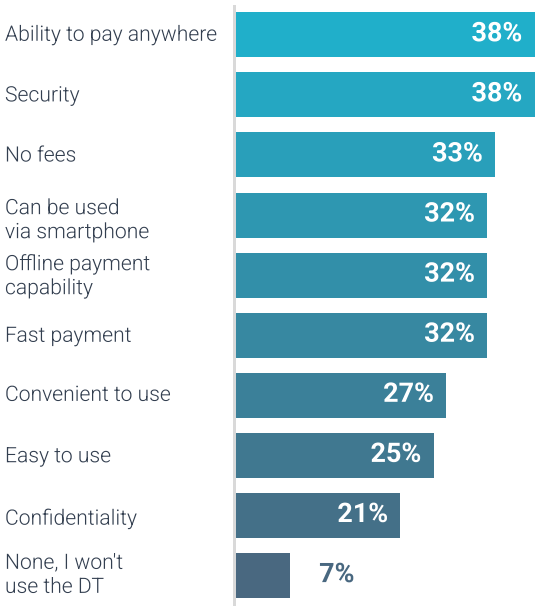
The least ready to use the DT are those who feel uncomfortable using cashless methods

Acceptance of the DT after the note with the DT's properties decription depending on the payment methods' convenience

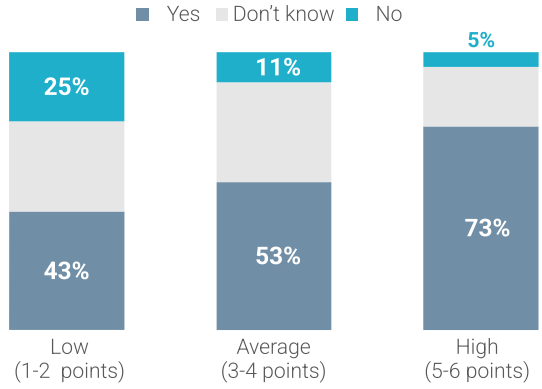


All 17 regions of Kazakhstan

Most important characteristics of the DT

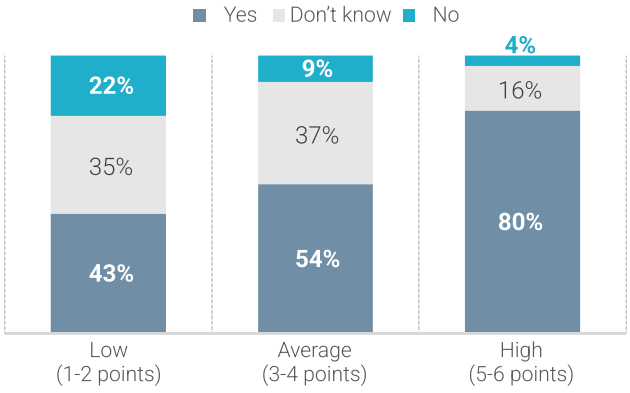


Acceptance of the DT after the note with the DT's properties description depending on the respondents' degree of trust in their bank



THE RESPONDENTS' DEGREE OF TRUST IN THEIR BANK

Acceptance of the DT after the note with the DT properties description depending on the respondents' degree of trust in the NBK



THE RESPONDENTS' DEGREE OF TRUST IN NBK

To what extent are market participants interested in the DT's further development and what percentage of scenarios can be completed within the DT Hub?

The approach to assess the potential of the DT ecosystem's creation implied that particular attention should be given to open communication with the market and its full involvement in the research process. Since the beginning of this year, numerous meetings and design sessions have been held. In particular, during such meetings, the results of the DT pilot project for 2021 were presented, and the goals and objectives of the second piloting phase for 2022 were outlined.

To encourage the interaction between financial market participants, independent experts, technology providers, and international partners and to develop the DT's ecosystem, the collaborative platform known as Digital Tenge Hub was created in June 2022. Within the DT Hub, all communications and stakeholders' interactions were carried out for joint research of the national digital currency implementation and its further development. For example, memorandums of understanding between the NBK and Digital Euro Association, the National Bank of the Kyrgyz Republic, and some technology providers have been signed within the DT Hub's operation.

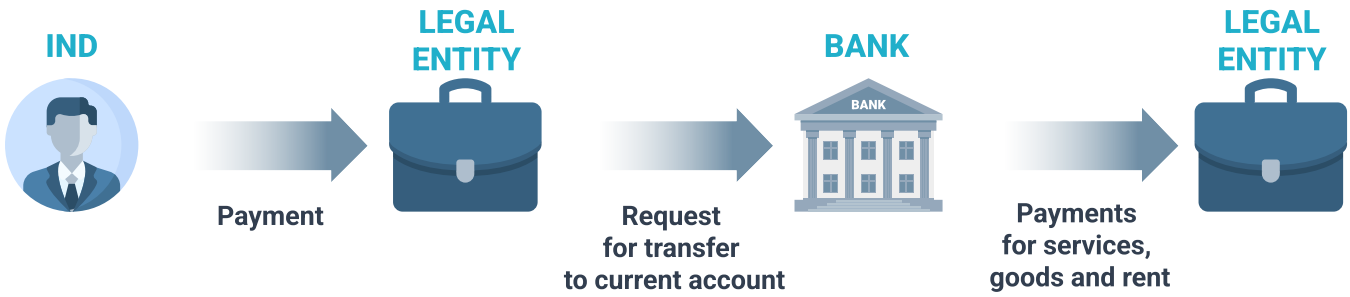
Participation in the Hub's activities gives several advantages, such as creating new experimental services on the DT platform to attract new customers, writing test smart contracts, training developers according to international standards, sharing experience, obtaining advice from foreign partners and experts, as well as access to the technological DT sandbox for experiments and joint case studies focused on the CBDCs' technical issues analysis.

One of the most important events at the DT Hub was the Ideathon which was held with market participants to identify a value proposition for end users. The competition's main goal was to understand the market's level of interest and awareness of the new payment scenarios that can be done via the DT. According to the competition's results, market participants proposed 17 innovative services for possible implementation on the DT platform. Received applications were selected with the use of the following criteria:

- benefits for consumers
- benefits for the state and business
- scenario's novelty (compared to existing ones)
- use of the DT's programmability features
- preservation of the existing payment system's two-tier model
- compliance with the smart contracts' requirements

All received applications were divided into three groups. The main criteria for selecting the first group of participants were the possible speed of their scenarios' implementation and the required functionality. The second group included scenarios with strategic benefits for the state, business, and consumers and prospects for the DT ecosystem development beyond the payment and settlement functionality. The third group's projects could demonstrate the DT's programmability and expand the range of scenarios for the use of the DT in the payment and settlement infrastructure.

“Transaction settlement between legal entities” scenario

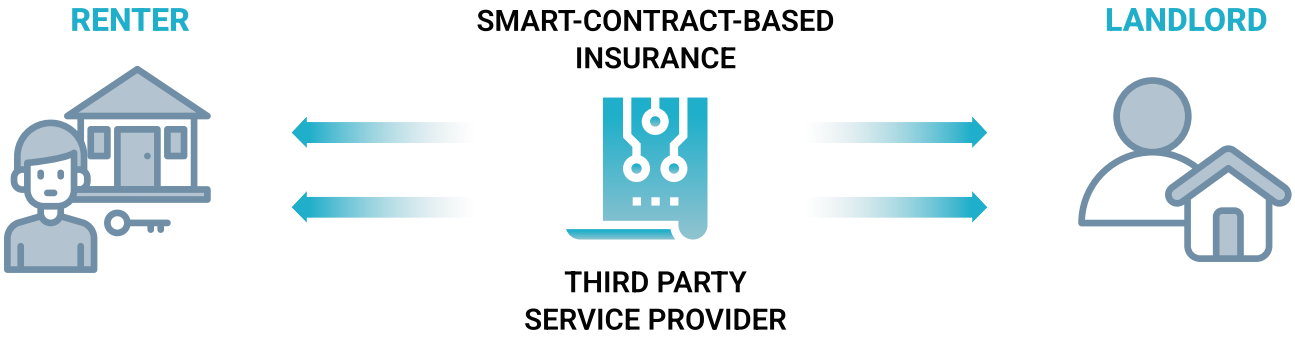


LIMITATIONS
Dependence on banks’ working hours
Operations’ duration
Cash gap risk
Risk of failure to meet deadlines

ADVANTAGES
Instant settlement
24/7/365 payment option
No delays
Token marking

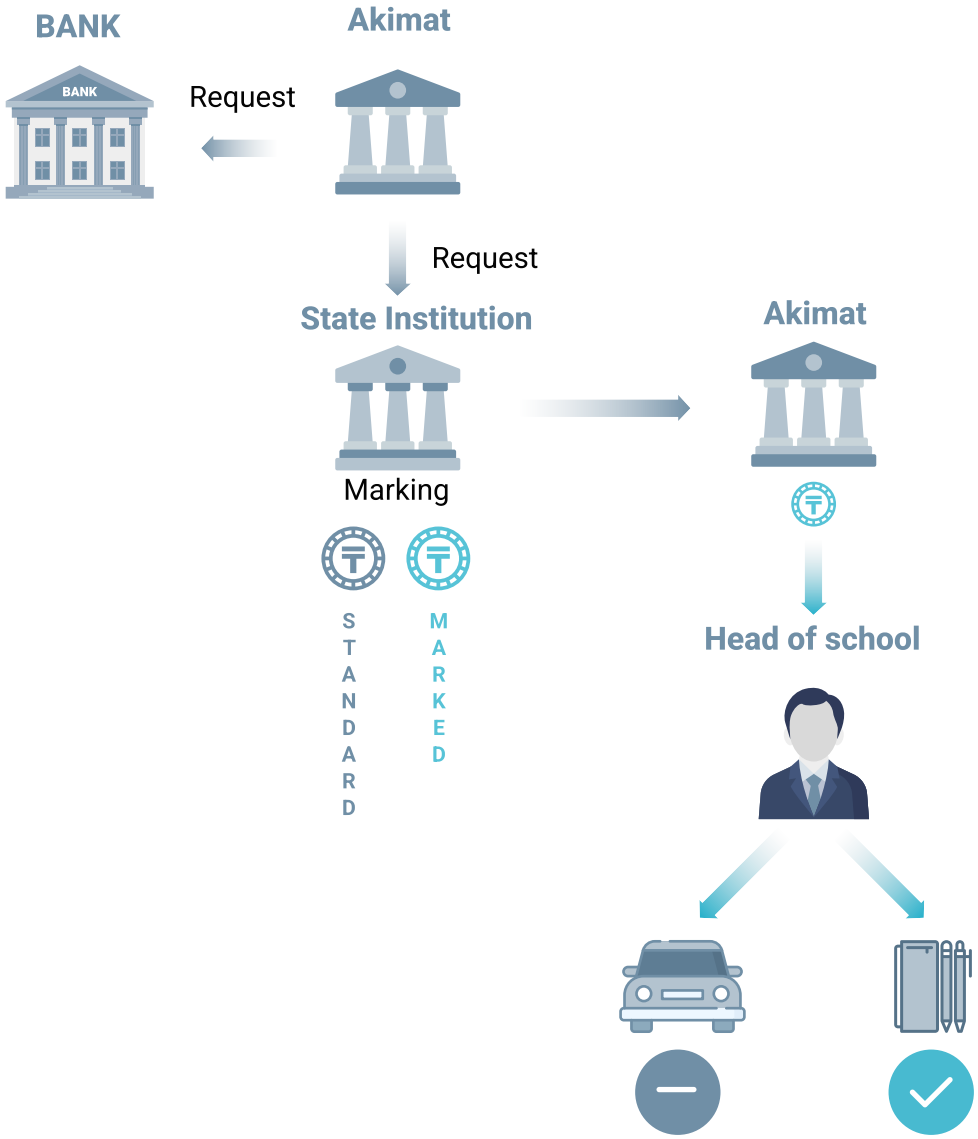
“Rental sector automation” scenario

HIGH RISKS
No financial obligations
No legal obligations
No guarantees
Unregulated increase in prices



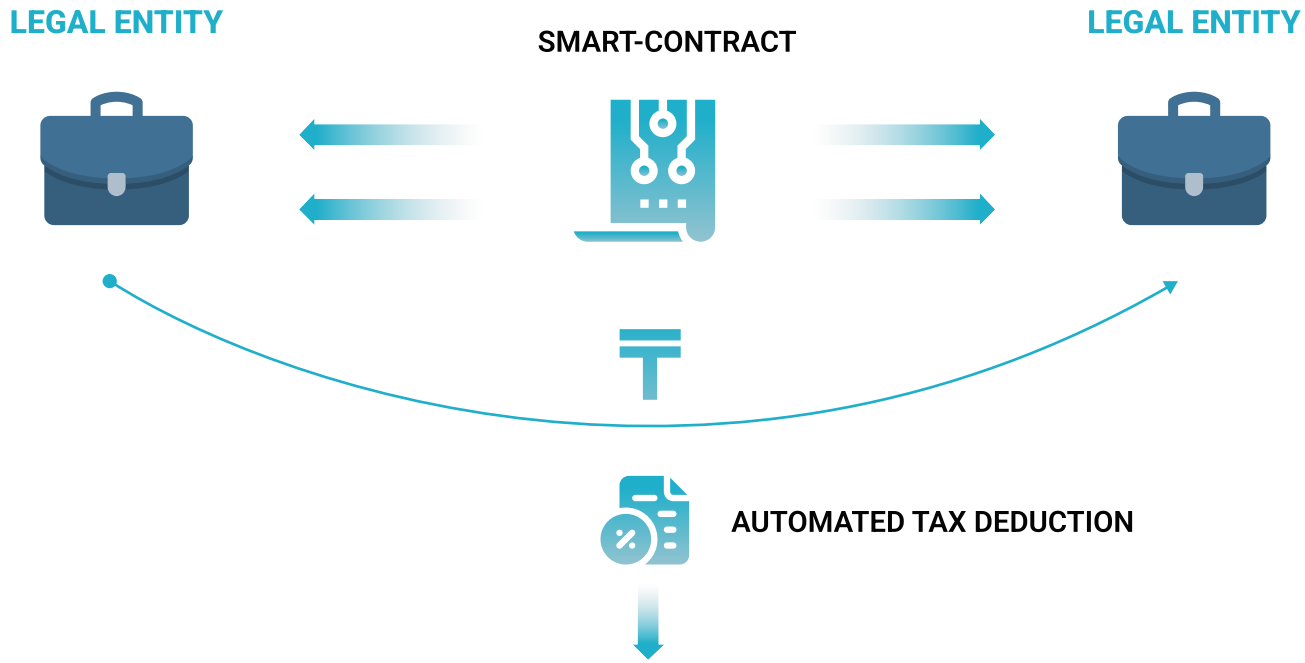
ADVANTAGES
Guranteed client’s solvency
Payment conducted in time
Automated process
Deferment of payment
Force majeure insurance
Insurance hold on both side: • *Landlord’s losses compensation* • *Guaranteed contract for Renter*

“Social assistance distribution system for socially vulnerable segments of the population” scenario



ADVANTAGES
Getting social assistance in time from a single window
Marking of tokens (use of funds for the intended purpose)
Automated process
Transparent social assistance processes
Current processes digital tranformation
No need to create an additional special account *(marked and standard tokens are stored in a single wallet)*

“Tax payment automation” scenario

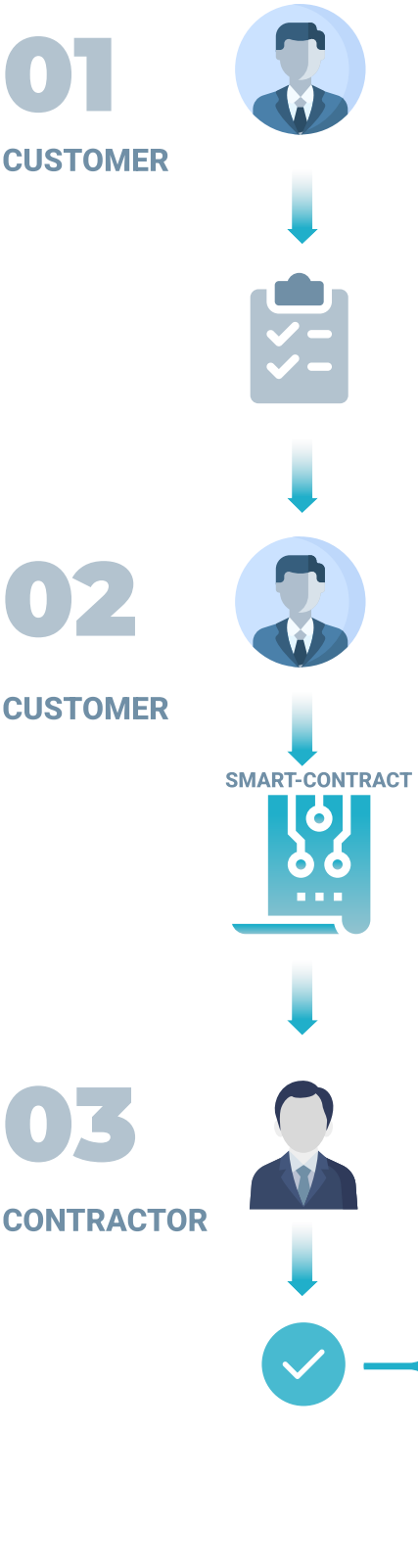


ADVANTAGES
Automated tax calculation and payment
Automated businesses’/GAs’ work
Option of tax regime selection
Business simplification
No tax debts

Among the proposed initiatives, there were promising scenarios for automating tax reporting using new smart contracts. Another unique idea was implementing an automated recruiting service on the blockchain, providing all measurable conditions and agreements. In addition, this service creates supply and demand information (vacancies) in the form of a smart contract. Smart contracts protect payments and taxes in this service in conjunction with DLT which brings strategic benefits to the population, government, and business.

Also, there were innovative proposals focused on solving problems of entering into lease contracts, hiring, and providing services using DLT technologies. One of the scenarios was aimed at creating an ecosystem in the form of a single digital platform for automating, registering, and digitalizing all processes of the rental industry in the RK. Some authors suggested paying wages in the DT which could automate processes and reduce the number of tax deductions and calculation errors. Another promising scenario was “Transaction settlement between legal entities” - the ability to make instant settlements in 24/7/365 mode could create unique value for many consumers. See the infographic at the end of this section to learn more about these and other scenarios.

“Safe deal” scenario



ADVANTAGES
Protected settlements between participants
Transparency of all transaction stages
Guaranteed payment on time
Full/partial transaction automation
Simplified tax collection process
Decreased number of conflict situations

The NBK has implemented the scenario that won first place among the first group’s participants, namely **the “Safe Deal” scenario** for automating settlements for freelance services. Currently, the NBK is also conducting training sessions based on the results of the development and implementation of smart contracts.

The "Safe Deal" scenario is a tool that helps to secure transactions between participants. All secure transaction stages and the use of the DT are as transparent as possible: the contractor does not doubt that the customer has the funds to pay for the order. In contrast, the customer controls the payment to the contractor's account. The transaction can be partially automated: for example, the payment can occur automatically after a certain time. Additionally, the secure transaction service can simplify the collection process and reduce conflict situations, which is also beneficial for the state.

Market participants have a stable interest in the DT platform

The Ideation's results show that market participants have a stable interest in the DT platform. Even in the conditions of a short time for preparation (14 days) and a relatively low level of awareness of the digital currency mentioned above, market participants presented 17 possible innovative scenarios for using the digital currency platform. It is also important to note the trend of increasing awareness among the fintech market's representatives - compared to the data of interviews with Kazakhstani banks' representatives in 2021. It can be stated that the level of immersion in issues related to the prospects of DT has increased significantly.

As a part of the last year's work on studying the potential of the DT's ecosystem, the 60 most relevant questions about the DT were collected from the representatives of several banks. The answers were sent to the banks and demonstrated at the meeting on September 17, 2021, followed by a discussion.

Evaluation findings

More than half of the market participants and consumers are ready and interested in the implementation and further development of the DT

The combination of all mentioned factors and answers to the Model's questions led to assigning **a "C" rating** to the DT platform's "Ecosystem" aspect (more than half of the market participants and consumers are ready and interested in the implementation and further development of the DT). Organizing works focused on increasing awareness among consumers and market participants are necessary to achieve higher values. And continue developing the ecosystem via events and meetings within the DT Hub. At the same time, the increased level of understanding and the DT Hub's efficiency should also be mentioned as positive trends that can be enhanced via further interactions with market participants.

It is necessary to organize works focused on increasing the level of awareness among consumers and market participants

OPERATIONAL MODEL

72-82
pp.

DT design

The operational model of a DT is a set of business processes, procedures, and regulations

The DT operational model is a set of business processes, procedures, and regulations aimed at legally defined, seamless, and mutually beneficial interaction between system participants.

Depending on each particular jurisdiction's motivations for implementing CBDC, the distribution of roles in the operational model will differ, and this process requires discussions with users and stakeholders. But the global consensus is that interoperability of CBDC at the national level will be key to the effective operation of the system. Interoperability will ensure coexistence of CBDC system with other national payment systems and promote greater accessibility, sustainability, and diversity of payment services.

Sustainable development of the ecosystem and achievement of the stated benefits of the DT in a two-tiered architecture is only possible with the involvement of market players and wide penetration into the consumer environment.

Sustainable development of the ecosystem and achievement of the stated benefits of the DT is only possible with the involvement of market players and broad consumer penetration

Hypotheses and research questions

The operational model consists of the following components which need to be defined as part of the study:

1. Allocation of roles, rights, responsibilities of the participants of the DT platform, requirements for the participants
2. Platform business model and charging approaches
3. Set of measures and approaches for dispute management
4. Approaches to the DT money scheme
5. Approaches to AML/CFT compliance management
6. Consolidation of the approaches in line with the legal acts
7. Model and approaches to achieve optimal level of the DT penetration

Assessment approach

The answers to the operational model questions were formulated by discussions with market participants at the DT Hub and analysis of international studies.

Study results

1. Allocation of roles, rights, responsibilities of the participants of the DT platform, requirements for the participants

The proposed operational model builds on the existing two-tier architecture where the NBK issues the DT, payment providers open wallets and distribute the DT on demand to the consumer. The model described allows to achieve a number of objectives such as increasing financial inclusion and maintaining financial stability. It also allows STB/FIs to access new revenues, which in turn will lead to a new evolutionary stage of financial market development in the country. According to a review of BIS, a basic division of roles in the DT system is proposed [35].

	List of roles	Basic allocation of functions and tasks
1	The NBK as a platform operator	**Core rulebook** The core principles of the DT transactions/use, outlining the legal basis, governance, risk management, access and other requirements of participants **Core infrastructure** Issuing, redeeming and settling the DT on the ledger and potentially monitoring, safeguard **Processing Infrastructure** Message preparation, processing and reconciliation, communication with core infrastructure, connectivity with enabling functions (eg digital identity systems, underlying telecoms networks)
2	Payment service providers	**Processing Services** Payment pre-checks (e.g., limit checks, funds availability) Authorisation, verification or validation (e.g., managing exceptions, restoring and correcting transactions, handling offline authorisation limits) Screening (e.g., security and regulatory checks) Data and analytical services **Payment Services (interaction with end users)** Pre-transaction (e.g., access device or channel, on-boarding of users) Transaction (e.g., payment instruction, authentication, customer service and support) Post-transaction (e.g., payment advice statements and billing)

	List of roles	Basic allocation of functions and tasks
2	Payment service providers	**Use case arrangements** A set of business and technical rules determining how a use case works
3	AML/CFT designated authority	**Processing Infrastructure** Connectivity with enabling functions (e.g., digital identity systems, underlying telecoms networks)
4	GA that programs tokens	**Use case arrangements** A set of business and technical rules determining how a use case works

The approach to developing requirements is similar to systemically significant payment systems' requirements. The operational model described does not require the cost of connecting to the DT platform more than existing mechanisms and regulations do.

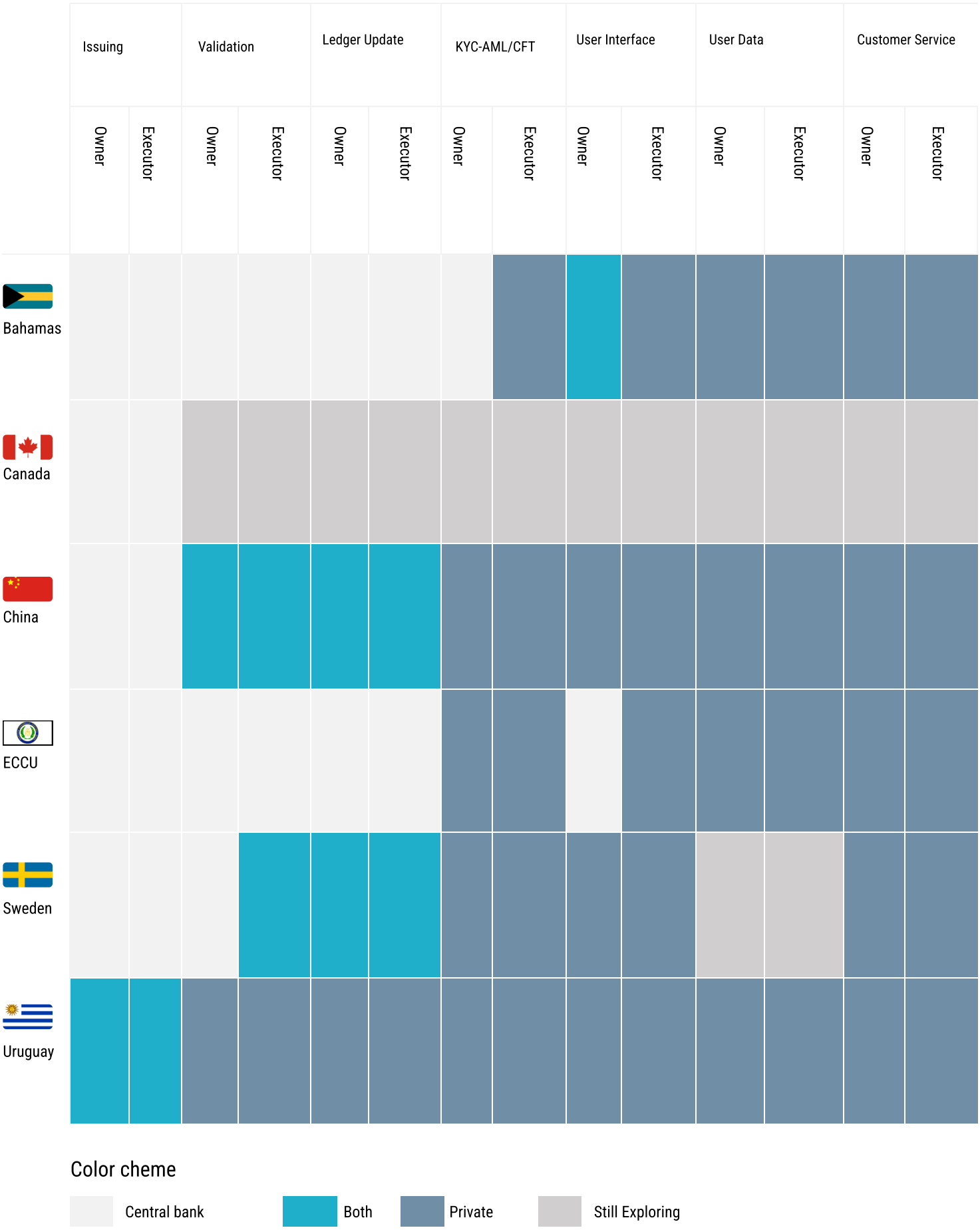
The allocation of functions and tasks between the roles may vary depending on the DT scenario

The allocation of functions and tasks between the roles may vary depending on the DT scenario. The results of the pilot demonstrated minimal costs for integration with the DT platform on the side of the market participants (minimum refinements).

Regardless of the design, developing and launching a CBDC system will be a challenge for any central bank. Any functions outsourced should be carefully designed to ensure public confidence in the CBDC system. Similarly, individual and collective oversight of those functions and services provided or managed by private intermediaries will be required.

Further roles and functions require detalization in line with the planned tasks in the 2023 scenarios

Further roles and functions require detalization in line with the planned tasks in the 2023 scenarios. The proposed approaches will be tested in the regulatory sandbox of the NBK along with all market participants.



Source: IMF [33]

ECCU- Eastern Caribbean Currency Union

2. Platform business model and charging approaches

Approaches of foreign regulators

A review of a number of CBDC projects:

Central Bank of the Bahamas (where the digital currency has been launched), People's Bank of China, Eastern Caribbean Central Bank and Central Bank of Uruguay (where pilot projects with real consumers and merchants have been and continue to be conducted), Riksbank (where the digital currency is being reviewed by government or parliamentary bodies outside the central bank), Bank of Canada (where the CB has conducted a digital currency project and decided not to issue a digital currency yet).

The review revealed the following conclusions about the approach of foreign regulators [33].

Access to and processing of payment data will play an important role in any ecosystem. Privacy issues can create a number of other design and interoperability challenges, ranging from the messaging standards used, creating incentives for different intermediaries to offer services, and interacting with traditional systems that require detailed account and transaction information [36].

The People's Bank of China (PBOC) notes it does not charge intermediaries or users, and intermediaries cannot charge individual users in the e-CNY project. However, intermediaries have the choice of charging merchants. The PBOC views this as a substantial incentive for firms to enter the market, and keeping fees in check.

The Bank of Canada states the choice of business model is complex. One possibility is for the central bank itself to provide a basic CBDC payment function to the public, possibly but not necessarily charging a fee for using it. The Riksbank is also considering this approach.

The question of whether a central bank should charge intermediaries for using the CBDC system is also connected to the question of whether it anticipates recovering its development costs. There is a risk that if central banks collect fees, intermediaries can pass the cost downstream and raise the price of payments which may counter initial policy goals. The question of whether and how to cover costs remains an open question, and the BOC states this as one of its most important areas of research.

Staff at the Riksbank also state that charging intermediaries fees is difficult because of the current regulatory framework. Another issue is that charging fees would possibly contradict its commitment to offering payments as a public good. Revenues for the central bank would likely solely be in the form of seignorage.

While subsidizing the adoption of CBDC is currently not seen as a viable path, the Riksbank is discussing if it might subsidize the cost of developing certain functions that the private sector would not find profitable. Examples of this include increasing payments resilience and developing payment solutions for minorities.

The NBK has identified the following key principles in developing a business model:

1. **The NBK is not interested in profit; the business model should only cover the costs of maintenance**
2. **Approaches to tariff setting should be developed on a win-win basis for all participants in the platform**

In order to determine the optimal operational model according to these principles the rules of the DT business model will be developed in the regulatory sandbox together with all participants in 2023.

3. Set of measures and approaches for dispute management

Safeguarding the interests of end-users is a key pillar of any payment system. It is important to provide safeguards to consumers in different scenarios. Market participants need to consider new ways to ensure consumers' protection when making payments with the DT[36]:

- an unauthorised payment (e.g. if a CBDC payment instrument, or a digital token, is stolen or lost)
- a fraudulent act that causes customer harm
- a fault in the service provided by the private sector PIP
- a fault with goods or services purchased

Issues related to the regulatory sandbox should be worked through in the tests:

- upfront costs of setting up new processes to receive, investigate and resolve claims and disputes
- ongoing costs of running the consumer protection framework

Based on the role model of the DT operational model, a taxonomy and algorithms for dispute resolution will be developed. The system will be automated.

4. Approaches to the DT money scheme

The money scheme is one way of recording and storing the state of a transaction. Eight variants of a monetary scheme for settlement are identified.

Monetary unit (what changes)	Value	Bearer	Identity of the unit	Explanation
Trivial	Fixed	Fixed	Fixed	The trivial scheme is very simple: a static money system in which no payment is possible
Bills	Fixed	Variable	Fixed	A €20 note with a unique serial number is handed from Alice to Bob or the ownership of a €20 digital bill is changed from Alice to Bob
Accounts	Variable	Fixed	Fixed	Alice's account is debited €20, Bob's is credited €20
UTXO	Variable	Variable	Variable	UTXOs are spent only once, and when this is done, new UTXOs are created with different identifiers. Alice's existing UTXO is destroyed, creating two new UTXOs, one belonging to Alice, and one new UTXO worth €20 belonging to Bob
Extended accounts	Variable	Variable	Fixed	The ownership of accounts can change
Variant 1	Fixed	Fixed	Variable	This scheme does not allow either the value or the owner of a monetary unit to change, so payment is not possible under this scheme
Variant 2	Fixed	Variable	Variable	This scheme is like a bill scheme, but the bill's serial number changes when it is spent; it does not offer much additional utility beyond the bill scheme
Variant 3	Variable	Fixed	Variable	This scheme is like an account scheme, but every payment results in a new account. It does not offer much more than the fixed identifier account does

Source: Guardtime [33]

Both bills and accounts have specific identifying numbers, with serial numbers for bills and account numbers, that do not change during the course of a payment.

The following three types are considered for CBDC [33]

Categories	Variants
Money scheme (data model)	Account, UTXO, Bills
Ledger type	Trusted machines, permissionless blockchain, permissioned DLT, centralised blockchain, offline
Transfer mechanism / bearer check	Identity-based authentication, token or signature-based authentication, smart contracts

The differences in the data structures of these monetary units mean the choice of monetary scheme may have an impact on many elements of the DT, including scalability, anonymity, the legal status of the monetary unit, and the security of the money supply. However, we can also identify characteristics of the DT that are frequently mentioned in the context of tokens or account and that are little affected by the choice of money scheme, including the availability and resilience of the system, the confidentiality of the ledger, and the security of the ledger. These are properly described as arising from the choice of bearer technology or ledger type.

The UTXO model was chosen for the DT because of its advantages in terms of anonymity, programming compared to other options. The balance sheet accounting model is described in more detail in the Final Report 2021.

Categories	Variants
Scalability and settlement time	The choice of monetary scheme affects the scalability of payments and determines the process by which settlement occurs. Ledger and bearer technology also have a strong impact on scalability and settlement time
Anonymity	An account contains a history of multiple transactions by the same user which makes it easier to use various analytical techniques to de-anonymise the identity of the account holder. If one transaction is de-anonymised, the entire payment history of that user can be identified **Bills and UTXOs make it easier to employ techniques that keep identities secret, such as transaction splitting and one-time addresses**
Legal status	Some existing legal frameworks for central bank money draw distinctions between accounts and bearer instruments or cash. Legal analysis by the IMF has indicated that a result of this may be that CBDC tokens are legally more permissible in some jurisdictions than accounts offered directly to the public are. More research is needed to determine whether these distinctions are primarily a function of the choice of bearer technology or money scheme

Categories	Variants
Interest bearing	Interest on account-based instruments is calculated periodically from the balance. If UTXOs or bills are aggregated in wallets, interest can be calculated at the wallet level in a similar way to how account-based interest is calculated. However, both UTXOs and bills allow the additional option of calculating interest from each unit transaction, or calculating remuneration from the specific period of ownership, meaning the age of the UTXO or the length of time that a bill was held by its previous owner
Limits	For bills and UTXOs, it is first necessary to calculate the overall value of an individual's holdings. While this does not prevent limits or caps from being applied to UTXOs and bills, it does negate the anonymity advantages of bills and UTXOs over accounts.a
Programmability	Programmable money is possible under all three money schemes, but the nature of the data object that is programmable changes. For accounts, the balance is programmable, as a smart contract makes a payment from the balance. **For UTXOs, both bearer and account are programmable, as a smart contract mints new UTXOs.** For bills, the bearer is programmable, as a smart contract transfers the bill to a new owner

Source: Guardtime [34]

5. Approaches to AML/CFT compliance management

The main challenges in ensuring the interoperability of CBDC platform relate to technical, commercial and legal issues.

Legal/regulatory domestic barriers could include differences arising from participant supervisory regimes and compliance requirements as well as settlement finality and consumer protection rules in payment systems. Specifically, if there were different supervisory requirements between a CBDC and other payment systems then there could be insufficient overlap to ensure a smooth flow of funds (assuming a more technical interface were not implemented). Similarly, if know-your-customer, anti-money laundering and counter terrorism financing requirements were higher or differed from existing payment systems, this could add costs to participants. For payment systems, rules on the finality of settlement and consumer protection could differ (eg where one system was net settlement and another was gross settlement and procedures in the event of transaction errors, delays, fraud, theft, or insolvency differed). As for other barriers, early engagement and dialogue would be essential to avoiding issues, in this context, with other public authorities tasked with bank and/or payment service provider supervision, the providers themselves and other payment systems..

Collaboration with other government agencies tasked with supervising banks, payment service providers and payment systems is essential to remove barriers. The NBK is committed to the principle that the requirements will be similar to the AML/CFT requirements of systemically important payment systems.

6. Consolidation of the approaches in line with the legal acts

The basic parameters of the operational model will be developed next year. Also, given the need to refine the interaction rules in the regulatory sandbox, further analyses will be carried out. The results of the 2022 regulatory study are summarised in the following chapter.

7. Model and approaches to achieve optimal level of the DT penetration

According to the Canvas pyramid previously described, the two-tier model of the DT design ensures that participants who are aware of specific consumer problems and pains are encouraged to create such innovative scenarios. In the process of learning about the DT, the key driver for creating an ecosystem is to select the right initial business cases for the phased implementation of the DT. Such scenarios should provide network effects, stimulate demand for the DT and, therefore, create a market for payment service providers.

The primary scenarios considered are X2G/G2X scenarios.

Ensuring interoperability between market participants' systems is one of the main challenges to building an efficient operational model. Interoperability between payment systems can promote competition among payment service providers, enable innovation and enhance the operational resilience of the national payment ecosystem. Low levels of interoperability between payment systems can lead to the fragmentation of the payment landscape into closed loops. As a result, users and merchants may face costs due to participation in restricted systems, which reduces the speed and increases the cost of payments.

Technical barriers could include: inconsistent standards for message formats, data elements, numbering and coding systems, security protocols, scalability or throughput capacity and opening hours.

Avoiding these barriers could involve, respectively: using of common (international) technical standards and/or application programming interfaces; requiring minimally viable security standards or encouraging other systems to adopt stronger security; engaging in early and frequent communication with other systems to estimate volumes and throughput; and establishing rules for CBDC payments initiated during the closing hours of other systems. relevant stakeholders could agree a CBDC's technical specifications and coordinate interoperability issues.

Commercial barriers could include an unwillingness of other systems and/or participants to use the CBDC to protect revenues from existing systems. In response a central bank could incentivise participation in the CBDC ecosystem and engage in early outreach. Lowering costs by avoiding the technical interoperability barriers above could also help.

Evaluation findings

The distribution of roles and tasks among the roles may vary depending on the DT scenario

The proposed operational model builds on the existing two-tier architecture, where the NBK issues the DT, payment providers open wallets and distribute the DT on demand to the consumer. The distribution of roles and tasks among the roles may vary depending on the DT scenario. **The UTXO model was chosen for the DT because of the advantages in terms of anonymity, programming compared to other options.**

The results of the study showed low regulatory costs

The results of the study showed low regulatory costs for the following reasons:

- The technological, regulatory requirements for market participants to connect to the DT system will be similar to the existing requirements of systemically important payment platforms. Pilot results showed minimal costs for integration with the DT platform on the side of market participants (minimum refinements)
- The monitoring and supervision of the system will be automated using smart contracts. Taxonomy and algorithms for dispute resolution will be developed based on the role model of the operational model of the DT
- No damage to the basic business models of the STB is expected

No damage to the basic business models of the STB is expected

The latter is possible because:

- economic studies didn't revealed risks of flow of funds in current accounts to the DT
- there are instruments to control the flow of funds into the DT - limits
- new services/products with DT can be commercialised

Incentives to connect to the DT platform will not affect the funds of market participants.

The proposed approaches will be tested in a regulatory sandbox by the NBK together with all market participants

Further roles and functions require detalization in line with the planned tasks in the 2023 scenarios. The proposed approaches will be tested in the regulatory sandbox of the NBK together with all market participants.

REGULATION

84-89
pp.

DT design

The legal status of digital currency is critical for its functioning as a component of the national payment system. It predetermines the digital currency's acceptance by the population and influences the choice of possible business cases for implementation on the platform. However, formulating recommendations for required changes in legal acts is complicated due to the digital currencies' novelty: the current legal framework does not consider any legal means of payment other than banknotes and coins.

The DT must be a legal tender in the territory of the RK, thereby ensuring the widespread acceptance of DT as a payment tool for goods and services

In 2022, research on the relevant laws and codes of the RK was conducted to determine the extent of the necessary changes, as well as their nature. During the process of developing mechanisms for regulating the possible implementation of the DT and its circulation, the following aspects were identified:

1. The DT will combine some features of cash and non-cash payment instruments
2. The NBK will have the exclusive competence to issue the DT and to control the DT's system functioning
3. The DT's face value must be equal to that of the ordinary Kazakhstani tenge, and DT must be legal tender in the territory of the RK, thereby ensuring the widespread acceptance of DT as a payment tool for goods and services
4. The DT will be an obligation of the NBK (will act as a guarantor)

Hypotheses and research questions

The research conducted during the analysis of possible options for the operational model resulted in a list of the most critical questions, and the answers were crucial for clarifying the most fundamental aspects of the entire life cycle of the DT:

1. What is the most appropriate definition of DT?
2. Is the DT subject to property or liability rights?
3. What does the circulation of the DT include?
4. What actors participate in the circulation of the DT?
5. How should the perception of personal data and banking secrecy change after implementating of the DT?
6. How should responsibility for the wrongful actions in the circulation process be differentiated (both administrative-legal and criminal)?
7. What qualifying should signs of wrongful actions be highlighted?
8. How should the AML/CFT procedures change during the implementation of the DT?
9. What restrictions should be set in the circulation of the DT (by the circle of persons and by the nature of the transaction)?

The information below describes proposed changes in the legislation of the RK including answers to the questions above.

Assessment approach

The creation of recommendations for the legal acts changes consisted of the following stages:

- Analysis of existing approaches to the creation of CBDC-oriented regulatory and legal framework
- Analysis of the RK's legislation for its relevance and correlation with each stage of the DT's life cycle
- Creation of recommendations with respect to obtained information

The combination of the steps above is an example of a standard gap analysis. This approach is a common one for identifying necessary changes in the legal framework.

Study results

The results of the completed analysis of the DT-related regulation can be found in the comparative table given in Appendix 3.

In 2022, the analysis of the regulatory aspects related to digital currency implementation in other countries was conducted, but the findings of the 2021 final report were similar. The lack of changes may be explained by the relatively small number of objects of study. There are only 4 CBs that have implemented digital currency as a payment instrument (Eastern Caribbean Central Bank, Central Bank of Nigeria, Central Bank of the Bahamas, and Bank of Jamaica) [37].

To ensure the required legal status of the DT, a number of terms and concepts to be legislated were identified via the analysis of existing RK legal acts.

The DT is the NBK's obligation issued in electronic form and distributed within the framework of a two-tier financial architecture jointly with market participants.

To legislate the concept of the "Digital Tenge", it is proposed to make appropriate additions to the Civil Code of the Republic of Kazakhstan and the Law of the Republic of Kazakhstan named "On Payments and Payment Systems".

The circulation of the DT consists of the issue, placement, storage, transfer, sale, purchase, and redemption of the DT.

To legally consolidate the concept of "the circulation of the DT", it is proposed to make appropriate additions to the Law of the Republic of Kazakhstan named "On Payments and Payment Systems".

The entities involved in the circulation of the DT are the NBK, the DT operator, STBs, individuals, and organizations.

It is proposed to make additions and amendments to the following Laws and Codes of the Republic of Kazakhstan to legislate the rights, obligations, and responsibilities of entities involved in the circulation of the DT:

- "Payments and payment systems"
- "On the National Bank of the Republic of Kazakhstan"
- "On banks and banking activities in the Republic of Kazakhstan"
- "On personal data and their protection"
- "On standardization"
- "On currency regulation and currency control"
- "On rehabilitation and bankruptcy"
- "On counteraction of legalization (laundering) of incomes received by illegal means, and financing of terrorism"
- Administrative procedural and process-related code of the Republic of Kazakhstan
- Budget Code of the Republic of Kazakhstan
- Criminal Code of the Republic of Kazakhstan
- Entrepreneur Code of the Republic of Kazakhstan
- Tax Code of the Republic of Kazakhstan

There also may be additional changes in other laws and codes.

At the end of this section, there is a summary table that describes the directions of further work and principal legal differences between the DT and existing. Each of these directions and differences needs to be further elaborated as part of the objectives of developing the DT platform and determining its legal status.

It is also vital to mention specific difficulties arising in developing mechanisms for digital currency regulation. The reason for that is an ongoing legislative process to improve the legislation in digital assets. Within the working group, stakeholders expressed different points of view regarding the definition of terms, components of the digital asset circulation, and function distribution between the authorized bodies.

Moreover, the authorized body in the field of informatization has begun to develop the Concept of the Digital Code of the Republic of Kazakhstan, which in turn means a high probability of future revisions of this study's conclusions.

Direction	Conceptual differences of the DT
Definition of the DT	Non-cash payment instruments represent credit institutions' liabilities as bank accounts/deposits records The banknotes issued by the NBK presents cash The DT is the NBK's obligation, and there is a fundamental difference between non-cash instruments due to the information environment in which DTs are formed and used
Circulation of the DT	Marked tokens may be restricted in circulation New market participants' roles will be defined with respect to the DT's operational model
Technology New standards	The DT platform is based on hybrid technology: a combination of decentralized and centralized systems New cryptographic library of the DT platform New security standards New data standards for integration with other systems New standards for QR-codes, NFC protocol, and other transaction data transmission channels
Counterfeiting and loss of the DT-related data in private law	In case of the loss of the DT data in account-based CBDC (e.g., as a result of an accident), the user has the right to demand that the amount be returned to the account In case of the loss of the DT data in token-based CBDC, the monetary value is usually considered as a disappeared one. Therefore, the user cannot claim to reissue the funds, although this is technically feasible The discussion on the possibility of restoring funds in the DT system is still going on If the RK's law is amended to include digital currency counterfeiting/duplication as a currency counterfeiting offense, the specific characteristics of digital currency (level of difficulty in counterfeiting/duplication on a large scale within a short time) would also need to be considered and to be reflected by the law

Directions	Conceptual differencts of the DT
Private law foreclosure of the DT	Foreclosures of account-based CBDCs can be handled in accordance with the existing private bank deposit foreclosure process due to its similarity to the requirements for deposits Foreclosures of token-based CBDCs require further discussion
Obtaining information in accordance with AML/CFT regulations	There may be different levels of data provision and AML/CFT screening to mitigate the “digital run” risks Moreover, the DT wallets can be made available to the general population through simplified verification processes to increase financial inclusion
Protection of personal information	The DT system provides access to users' personal data for the STB/EP, but not for the NBK As in the case of the existing payment architecture in the RK, the STB/EP has access to information related to individual transactions through the DT system. This includes individual attributes (person's name and date of birth), payment attributes (amount of money and payment date), and commercial attributes (optional; the name of goods/services purchased and their unit prices). The issue of responsibility distribution between the system participants and the availability of certain data within the platform also requires further elaboration

Evaluation findings

The DT implementation's effectiveness and its circulation's viability depend on the legal regulation mechanisms of the DT

The DT implementation's effectiveness and its circulation's viability depend on the legal regulation mechanisms of the DT, a clear definition of terminology, and components of the DT circulation in the legal field.

The roles of all entities involved in the circulation of the DT, their rights, obligations, and responsibilities should be distributed according to the logic of their functional purpose in the DT's life cycle, without duplication of functions and with clear deadlines, sequences of actions and responsibility for their violations.

The rules on responsibility for violations in the sphere of DT circulation should be adequate for the consequences of such violations. They should allow appropriate criminalization of the regulation. However, they should also be a sufficiently effective preventive measure.

The implementation of the DT will affect several regulated areas

The implementation of the DT will affect several regulated areas, which will require research and modify numerous backbone and sectoral legal acts.

Operational model should be enhanced with the use of regulatory sandbox

The analysis provided above gives the following answer: **the implementation of the DT will potentially lead to a low level of regulatory costs,** the operational model should be enhanced with the use of regulatory sandbox.

FINAL SCORE ROAD MAP

91-95
pp.

Final score

Based on the above, it is tentatively recommended to introduce the DT. At the same time, considering the need for technological refinements and development of the operational model, it is recommended to ensure a phased implementation over three years.

	Criteria	Preliminary finding
1	**Technological effect/advantages**	Feasible, requires substantial revision
2	**Technological risks**	Controllable, needs refinement (cybersecurity, bandwidth, etc.)
3	**Economic effect**	Neutral
4	**Economic risks**	Controllable, requires the development of appropriate regulation
5	**Market readiness**	Sufficiently high readiness on the side of external participants involved in the project
6	**Regulatory impact assessment**	Potentially low regulatory costs, requires refinement of the operational model
7	**Benefits and costs for stakeholders**	Benefits can exceed costs in the case of an effective operational model

Roadmap

The implementation of the DT project in 2022 determined the key design parameters of the DT, tested the DT functionality on real users, and confirmed the technological feasibility of the new unique properties of the CBDC.

PRELIMINARY APPROACH TO THE ROADMAP VISION UP TO 2025

PROJECT STAGE

PILOTING

PROOF-OF-CONCEPT

PILOT WITH A LIMITED NUMBER OF PARTICIPANTS

CBDC IMPLEMENTATION

LAUNCHING THE TARGET PLATFORM

SCALING

DESCRIPTION

Prototype development to test the concept viability on limited functionality	**Prototype modification** and launch into trial operation with a limited number of participants	**Solution development** for launching into production level	**Adding** participants, creating new services and cross-border **integration**
July 2021 - December 2021	January 2022 – December 2022	January 2023 - December 2024	Up to December 2025

TARGET TECHNOLOGICAL SOLUTION SELECTION

Target platform development

Implementation of **integrations** with external participants, other platforms, payment systems
Development of **non-functional requirements** (security, performance, etc.)

Scenarios and R&D development

Development **of scenarios for launching in the target platform** (social payments and state procurement)
Cross-border payment model design, **R&D experiments**

Elaboration of regulatory and operational models

Launching the target platform

Piloting and launching the DT platform in Kazakhstan (social payments, NBK public procurement, pilot with crypto exchanges)
Participants' experiments in R&D within the technological sandbox
Development of cross-border payments with other countries

Elaboration of regulatory acts

Scaling

Scaling of the developed target solution, including:
Adding new participants
Adding new innovative services
Cross-border integration with other countries
Stable offline

Roadmap

According to the project development roadmap, the main task for the development of the CBDC in the RK is the development of a production-grade platform (with financial institutions, government organizations, and other external participants integration) for launching into trial operation.

This includes:

Development and testing of the extended DT functionality, including:

- social payments from government agencies to the population (using social wallet)
- government procurement
- the new DT programmability scenarios (incl. smart contracts)
- exchange into other forms of money
- recovery, wallet blocking, etc.

Research of the wholesale DT, the study of the possibilities of making and testing cross-border payments with other countries.

Non-functional requirements for the target platform development (including requirements for information security, performance, etc.).

Integration with:

- External participants and platforms
- National and international payment systems (including the DT conversion in other forms of money)
- National services.

Elaboration of regulatory and operational models (including the development of operational aspects of the CBDC functioning in Kazakhstan, macroeconomic modeling, and analysis of legal aspects of CBDC implementation).

Engagement of market participants involved with the Digital Tenge Hub to develop the DT platform jointly. R&D «technology sandbox» creation and development and testing of participants' scenarios.

«Last mile» solution choice (digital storage, cards, etc.) and offline payment method.

Approaches to the development of digital currencies in other countries

The implementation of national digital currencies is the focus of central banks worldwide. According to CBDC Tracker statistics, 91 central banks worldwide are exploring digital currencies, and 29 central banks are in the process of piloting digital currencies. One of the key trends in the world is the exploration of cross-border payments using digital currencies (Jura, mBridge, Dunbar, Icebreaker projects, and others). Below are countries that have made significant progress in developing retail digital currencies.

Projects for the development of CBDC in other countries

Country	Current status	Key Features	Future development
China [49-53]	Flow > 13 billion $ Provinces > 15 Individuals > 250 million Merchants > 5 million Number of transactions > 360 million Cross-border payments project (mBridge)	One wallet in one bank (+additional sub-wallets) Anonymity approach: anonymity for small amounts and traceability for large amounts Offline transactions	Use of e-CNY in corporate settlements, taxation, and government payments Launching cross-border payments with Hong Kong Exploring cross-border payments with BIS
Sweden [54-56]	The second phase of the project (with two external participants) has been implemented The third phase of the project is in progress	Testing of offline functionality Testing of integration with POS terminals Different models of token storage Various types of wallets (including anonymous wallets for small amounts)	Phase 3 of the project, main tasks: Exploring the programmability of money Interaction with external participants Legal status of e-krona Evaluation and selection of a technological solution
Russia [57, 58]	In 2022, a prototype of the digital ruble platform (involving 15 commercial banks) is being tested, and legislation is being developed to implement	Access to the wallet through any financial institution where the client is served Offline research No anonymity	2023 – piloting "real money" settlements (C2B, B2C). Creation of smart contracts on the platform 2024 – phased integration to the platform of all credit institutions, payments with government participation (C2G, B2G, G2C, G2B),

Country	Current status	Key Features	Future development
Russia [57, 58]			cooperation with other Central Banks for cross-border and currency exchange transactions 2025 – implementation of offline mode, the connection of non-bank financial intermediaries, financial platforms
EU [59, 60]	Research Phase (2021-2023) The aim is to work through design issues and distribution model for final users	Offline (under development, possible limits on offline wallets) Controlled anonymity (no fully anonymous wallets) Limits on the maximum amount of CBDC on the wallet	Continued work on the design of the CBDC, including interaction with financial intermediaries, development of the distribution model, compensation, role model Involvement of stakeholders in the project 2023 – the decision to start the next stage (stage of development and testing of technological solution, business mechanisms)
USA [61, 62]	A presidential decree on cryptocurrencies and CBDC was issued. Pilot project launched with financial companies in a test environment	Offline (in progress)	Implementation of a pilot project. The project aims to increase the speed of transactions

REFERENCE LIST

97-100
pp.

REFERENCE LIST

Technology

1.Corda Documentation. URL: https://docs.r3.com/en/platform/corda/4.6/open-source/node-database-tables.html

2.ISO 20022 Financial Services - Universal financial industry message scheme

3.ISO/IEC 18004:2015 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification

4.People's Bank of China (2021). Progress Progress Progress Progress of Research Research Research Research & Development Development Development Development Development of E-CNY in China http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

5. Riksbank. (2022). E-krona pilot Phase 2 https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf

6. The Korea Economic Daily. (2022). Bank of Korea to test CBDC on Samsung devices, not on iPhone https://www.kedglobal.com/cryptocurrencies/newsView/ked202201250001

7.Банк России. (2021). Концепция цифрового рубля. https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf

8. Модель принятия решений о внедрении Цифрового Тенге. (2022). https://payfintech.kz/digital-tenge

9. СТ РК 3712-2021. Код штриховой (QR-код), присваиваемый поставщиком платежных услуг или оператором платежной системы для осуществления платежей за предоставленные товары, работы или услуги в рамках предпринимательской деятельности

Economics

10.Abilov, N. (2021). A Medium-Scale Bayesian DSGE Model for Kazakhstan with incomplete exchange rate pass-through. International Economic Journal, Vol. 35(4), pp. 486-522. https://doi.org/10.1080/10168737.2021.1999298doi: 10.1080/10168737.2021.1999298

11.Abilov, N. and S. Rahardja. (2022). Optimal fiscal rules in a resource-rich economy. World Bank Policy Research Working Papers, Work in progress.

12. Abramova, S., Bohme, R., Elsinger, H., Stix, H. & Summer, M. (2022). What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents. Oesterreichische Nationalbank Working Paper, 241.

13. Agénor, P.R. (2016). Optimal fiscal management of commodity price shocks. Journal of Development Economics, Vol. 122(C), pp. 183-196. https://doi.org/10.1016/j.jdeveco.2016.05.00510.1016/j.jdeveco.2016.05.005

14. Assenmacher, K., A. Berentsen, C. Brand and N. Lamersdorf. (2021). A unified framework for CBDC design: remuneration, collateral haircuts and quantity constraints. ECB Working Papers, No. 2578.

15.Bachetta, P. and E. Perazzi. (2021). CBDC as imperfect substitute for bank deposits: A macroeconomic perspective. Swiss Finance Institute Research Paper, No. 21-81.

16.Barrdear, J. and M. Kumhof. (2021). The macroeconomics of central bank digital currencies. Journal of Economic Dynamics and Control, Vol. 142, pp. 104148. https://doi.org/10.1016/j.jedc.2021.10414810.1016/j.jedc.2021.104148.

17.Bijlsma, M., Cruijsen, C., Jonker, N. & Reijerink, J. (2021). What triggers consumer adoption of CBDC? De Nederlandsche Bank Working Paper

18.Brunnermeier, M.K. and D. Niepelt. (2019). On the equivalence of private and public money. Journal of Monetary Economics, 106(C):pp. 27-41.

19.Burlon, L. C. Montes-Galdón, M.A. Munoz and F.Smets. (2022). The optimal quantity of CBDC in a bank-based economy. ECB Working Paper Series, No. 2689.

20.Chiu, J., M. Davoodalhosseini, J. H. Jiang, and Y. Zhu. (2019). Central bank digital currency and banking. Bank of Canada Staff Working Papers, No. 19-20.

21.George, A., T. Xie, and J. Alba. (2018). Central bank digital currency with adjustable interest rate in small open economies. Mimeo.

22.Gerali, A., S. Neri, L. Sessa amd F.M. Signoretti. (2010). Credit and Banking in a DSGE Model of the Euro Area. Journal of Development Economics, Vol. 42(s1), pp. 107-141. https://doi.org/10.1111/j.1538-4616.2010.00331.x10.1111/j.1538-4616.2010.00331.x

23.Huynh, K., Molnar, J., Shcherbakov, O. & Yu, Q. (2020). Demand for payment services and consumer welfare: the Introduction of a central bank digital currency. Bank of Canada working papers.

24.Kantar Public. (2022). Study on new digital payment methods. Kantar Public- commissioned by the European Central Bank

25.Kim, Y.S. and O. Kwon (2019) Central Bank Digital Currency and Financial Stability. Bank of Korea Working Paper No. 2019-6. http://papers.bok.or.kr/RePEc_attach/wpaper/english/wp-2019-6.pdfhttp://papers.bok.or.kr/RePEc_attach/wpaper/english/wp-2019-6.pdf

26.Konebayev, E. (2020). Estimation of a Small Open Economy DSGE Model for Kazakhstan. NAC Analytica Working Paper, No. 6.

27.Kumhof, M. and C. Noone. (2021) Central bank digital currencies - design principles for financial stability. Economic Analysis and Policy, Vol. 71, pp. 553-572. https://doi.org/10.1016/j.eap.2021.06.012doi:10.1016/j.eap.2021.06.012.

28.Li, J. (2021). Predicting the Demand for Central Bank Digital Currency: A Structural Analysis with Survey Data. Conditionally accepted by Journal of Monetary Economics.

29.Minesso, M.F., A. Mehl and L. Stracca. (2022). Central bank digital currency in an open economy. Journal of Monetary Economics, Vol. 127, pp. 54-68. https://doi.org/10.1016/j.jmoneco.2022.02.001doi:10.1016/j.jmoneco.2022.02.001

30.Nyffenegger, R. (2022) Central Bank Digital Currency and Bank Intermediation with Heterogeneous Bank Deposits. University of Zurich Working Paper No. 409. https://www.econ.uzh.ch/static/wp/econwp409.pdf

31. OMFIF. (2020). Digital Currencies. A question of trust. OMFIF Report, Official Monetary and Financial Institutions Forum

Ecosystem

32. A. Arauz, R. Garratt, Diego F. Ramos F., Dinero Electrónico: The rise and fall of Ecuador's central bank digital currency, Latin American Journal of Central Banking, vol. 2, issue 2, June 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666143821000107#fig0001 [Accessed: 06-Jun-2022].

Operational model

33. Gabriel Soderberg in collaboration with Marianne Bechara, Wouter Bossu, Natasha Che, Sonja Davidovic, John Kiff, Inutu Lukonga, Tommaso Mancini-Griffoli, Tao Sun, and Akihiro Yoshinaga, February 2022, Behind the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons

34. Ahto Buldas, Märt Saarepera, Jamie Steiner, Luukas Ilves (Guardtime), Rainer Olt, Tiit Meidla (Eesti Pank), December 2021, A formal model of money schemes and their implications for central bank digital currencies

35. BIS, Central bank digital currencies: system design and interoperability, September 2021

36. UK Finance, Commercial models of a potential UK retail CBDC

Regulation

37. Atlantic Council's CBDC tracker

38. Civil Code of the Republic of Kazakhstan

39. Administrative procedural and process-related code of the Republic of Kazakhstan

40. Budget Code of the Republic of Kazakhstan

41. Criminal Code of the Republic of Kazakhstan

42. Entrepreneur Code of the Republic of Kazakhstan

43. The law of the Republic of Kazakhstan named as "Payments and payment systems"

44. The law of the Republic of Kazakhstan named as "On the National Bank of the Republic of Kazakhstan"

45. The law of the Republic of Kazakhstan named as "On banks and banking activities in the Republic of Kazakhstan"

46. The law of the Republic of Kazakhstan named as "On personal data and their protection"

47. The law of the Republic of Kazakhstan named as "On standardization"

48.The law of the Republic of Kazakhstan named as "On currency regulation and currency control"

49. The law of the Republic of Kazakhstan named as “On rehabilitation and bankruptcy”

50. The law of the Republic of Kazakhstan named as “On counteraction of legalization (laundering) of incomes received by illegal means, and financing of terrorism”

Road map: overview of countries

51. People's Bank of China (2021). Progress Progress Progress Progress of Research Research Research Research & Development Development Development Development of E-CNY in China http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

52. China’s financial system https://www.economist.com/finance-and-economics/2022/09/05/the-digital-yuan-offers-china-a-way-to-dodge-the-dollar

53. China's digital currency passes 100 bln yuan in spending – PBOC https://www.reuters.com/markets/currencies/chinas-digital-currency-passes-100-bln-yuan-spending-pboc-2022-10-13/

54. Bank of China: Digital yuan transactions volume crossed $14B mark Bank of China: Digital yuan transactions volume crossed $14B mark (cointelegraph.com)

55. Details about the digital yuan wallet officially disclosed - Ledger Insights - blockchain for enterprise

https://www.ledgerinsights.com/details-about-the-digital-yuan-wallet-officially-disclosed/

56. Riksbank. (2021). E-krona pilot Phase 1

https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf

57. Riksbank. (2022). E-krona pilot Phase 2

https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf

58. Riksbank https://www.riksbank.se/en-gb/payments--cash/e-krona/

59. Сайт Банка России (2021) http://www.cbr.ru/fintech/dr/#highlight=%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9%7C%D1%80%D1%83%D0%B1%D0%BB%D1%8C%7C%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%7C%D1%80%D1%83%D0%B1%D0%BB%D1%8F

60. Основные направления единой государственной денежно-кредитной политики на 2023 год и период 2024 и 2025 годов https://cbr.ru/Content/Document/File/139691/on_2023(2024-2025).pdf

61. Progress on the investigation phase of a digital euro https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf

62. Digital euro legislation planned for 2023 https://www.ledgerinsights.com/digital-euro-legislation-cbdc/

63. Banking giants and New York Fed start 12-week digital dollar pilot https://www.reuters.com/markets/currencies/banking-giants-new-york-fed-start-12-week-digital-dollar-pilot-2022-11-15/

64. Ensuring Responsible Development of Digital Assets https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets

65. BIS - Central bank digital currencies: financial stability implications September 2021

APPENDIX

102-145
pp.

Apendix 1

Scenario	Technological features
Opening wallets	Structural participants' wallets (FIs/EPs/GAs) are formed when nodes are deployed and connected to the network. The process of opening clients' wallets (individuals, merchants) is based on the creation of key pairs (private, public) by clients at the level of their devices and the registration of part of them on the member's node (FI/EP). Ownership of the keys allows the client to fully control operations with DT (only the client has part of the private key, which allows operations). Three wallet models have been tested.
Issuance and distribution to FIs/EPs or GAs	Token issuance is a unique transaction available only to the NBK, it ensures the reliability of the DT life cycle. Restrictions on the ability to perform issuance are achieved using a role model. All transactions used the Pedersen Commitment to hide the amounts in the transaction, as well as a Kernel signature, which certifies the formation of the commitment and proves that the hidden amounts are produced correctly. The peculiarity of the issuance transaction is that there is no input token.
Distribution to individuals (standard DT)	Since the client's wallet and FI/EP are linked to the same FI/EP, the transaction involves one FI/EP node and a notary node. Transactions are created where the recipients are individuals represented by the node of the serving FI/EP. During any transactions with tokens (transfer, purchase, and distribution), the mechanism of minimum token selection is activated to form the transaction amount.
Token marking	Possible types of special tokens with several types of restrictions are defined in advance (types of restrictions: by time, by quantity, by the recipient of DT). The registry of token types and their restrictions is stored on participants' nodes. Conditions for spending special tokens are requested by the client along with a balance request.
Distribution to individuals (special DT)	The special token distribution mechanism differs from the distribution of standard DTs in that it involves two nodes - the state institution node and the FI/EP node.
C2C transfer (via QR-code)	QR-code is used as a way of transferring details or payment details from one participant of the transaction to another. If the sender has chosen to hide the information, stealth values will be used during the transfer. Before sending a transaction initiation request to the client's node, the client side signs the transaction with his/her private key.
C2C transfer (via mobile phone number)	To transfer by phone number, a request is made to the alias registry (ID Center) to get the address of the customer's wallet and the name of the bank that supports the wallet. Hiding data and signing the transaction is like the C2C QR-code transfer scenario.

Scenario	Technological features
Purchase with the Standard DT	Transferring data about the recipient uses a QR code from the merchant to the client. Hiding data and signing the transaction occurs similarly to the C2C transfer scenario (by QR-code).
Purchase with the special DT	Transferring data about the recipient uses a QR code from the merchant to the client. Data hiding and transaction signing take place similarly to the C2C transfer scenario (by QR-code). At the node level, there is a check of the correctness of fulfillment of conditions inherent in this or that type of special DT.
Reissuance (including technical redemption)	The reissuance is conducted automatically (without the direct involvement of the client) in four consecutive transactions (issuance, distribution, transfer, and redemption).
Monitoring	To track the MVP indicators of the pilot platform, the collection, and processing by direction are implemented: • Monitoring of non-functional parameters during transactions. • Monitoring of infrastructure parameters of the MVP pilot platform. • In addition, a data showcase for building business intelligence has been organized.
Offline payments (with a chain of offline transactions)	Users' devices must be within the range of the NFC connection when performing offline transactions. When performing offline transactions, payment instructions are stored on the client's devices. When any of the transaction participants go online, all payment orders are sent from the device of the transaction participant (individuals and/or merchants) to the node of the FI/EP of the transaction participant, and the DTs are synchronized on the device and in the storage of the FI/EP's node. In the case of when the second participant of the transaction goes online, the same unconfirmed payment order is sent to the DT platform for the second time, but the transaction on the DT platform is performed only for the first payment order. The second time it is considered processed and ignored. Thus, the absence of multiple uses of tokens is guaranteed.

Individuals MVP

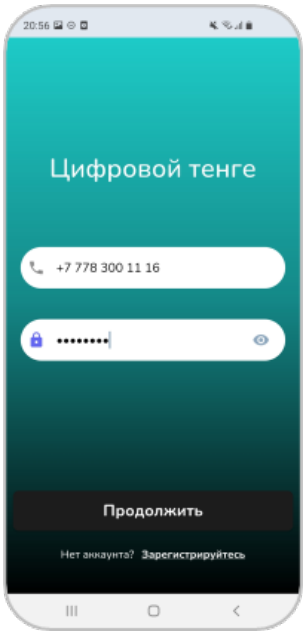
Opening wallets and distribution

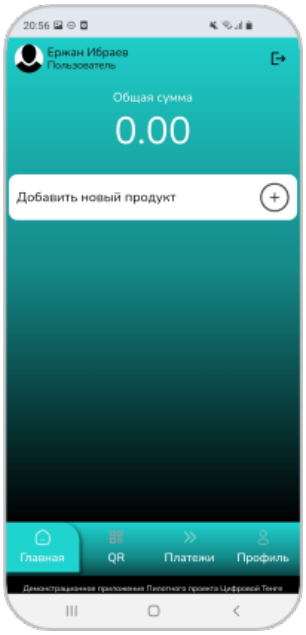
01 → Individual registers and logs in to the application

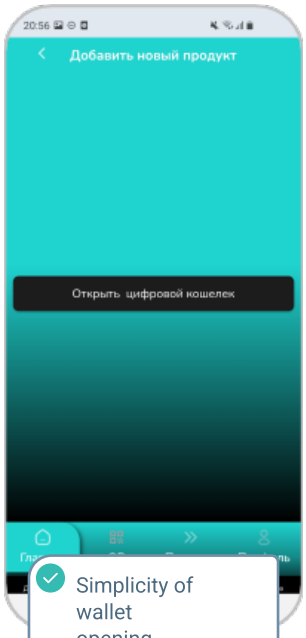
02 → Individual clicks “Open new product”

03 → Individual clicks “Open Digital Wallet”

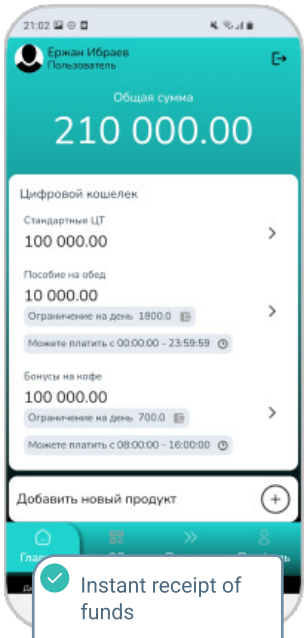
04 Individual sees his DT account details







Simplicity of wallet opening



Instant receipt of funds

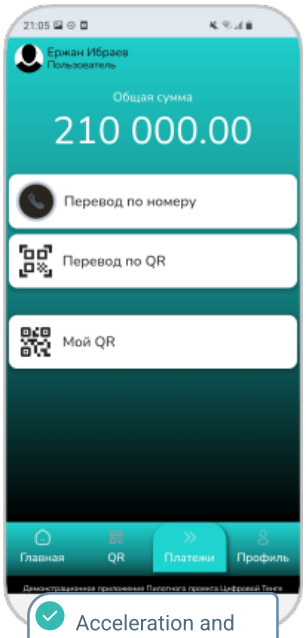
Transfers

05 → Individual clicks “Transfer”

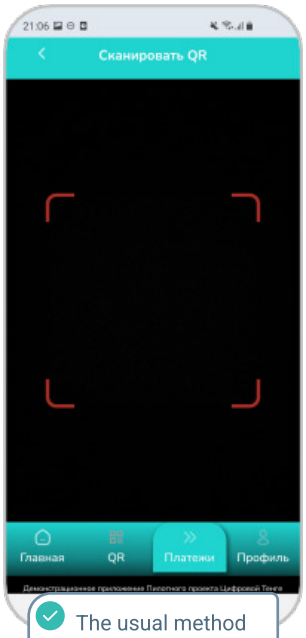
06 → Individual chooses «Transfer by QR-code», scans QR-code of another individual

07 → Individual enters the DT amount to transfer, confirms transaction

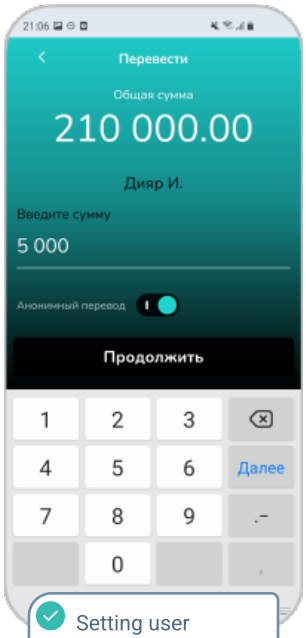
08 Individual chooses «Transfer by phone number», enters phone number and DT amount, confirms transaction



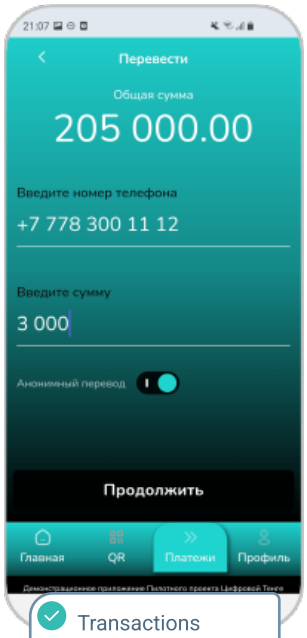
Acceleration and reduction of settlement risks



The usual method of payment by QR code



Setting user anonymity

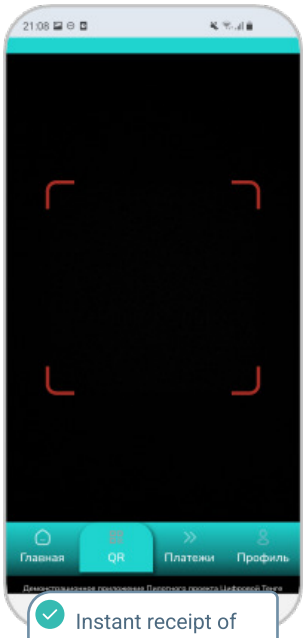


Transactions 24/7/365

Individuals MVP

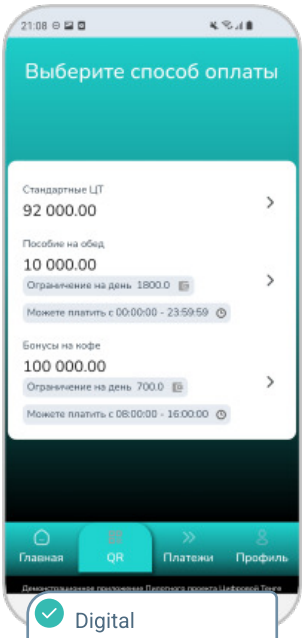
Purchase

09
Individual clicks «QR» , scans merchant's QR-code



Instant receipt of funds

10
Individual chooses DT type to pay

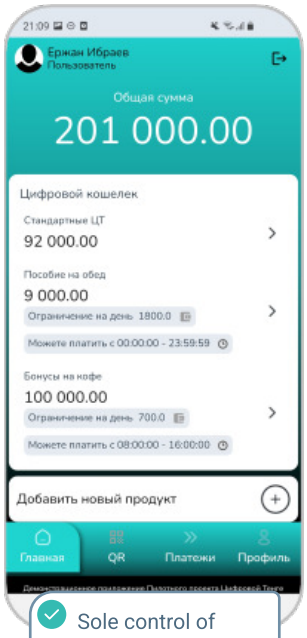


Digital alternative to cash

11
Individual checks information and confirms the transaction

Transaction security

12
Individual sees updated balance of digital wallet



Sole control of funds

Merchant MVP

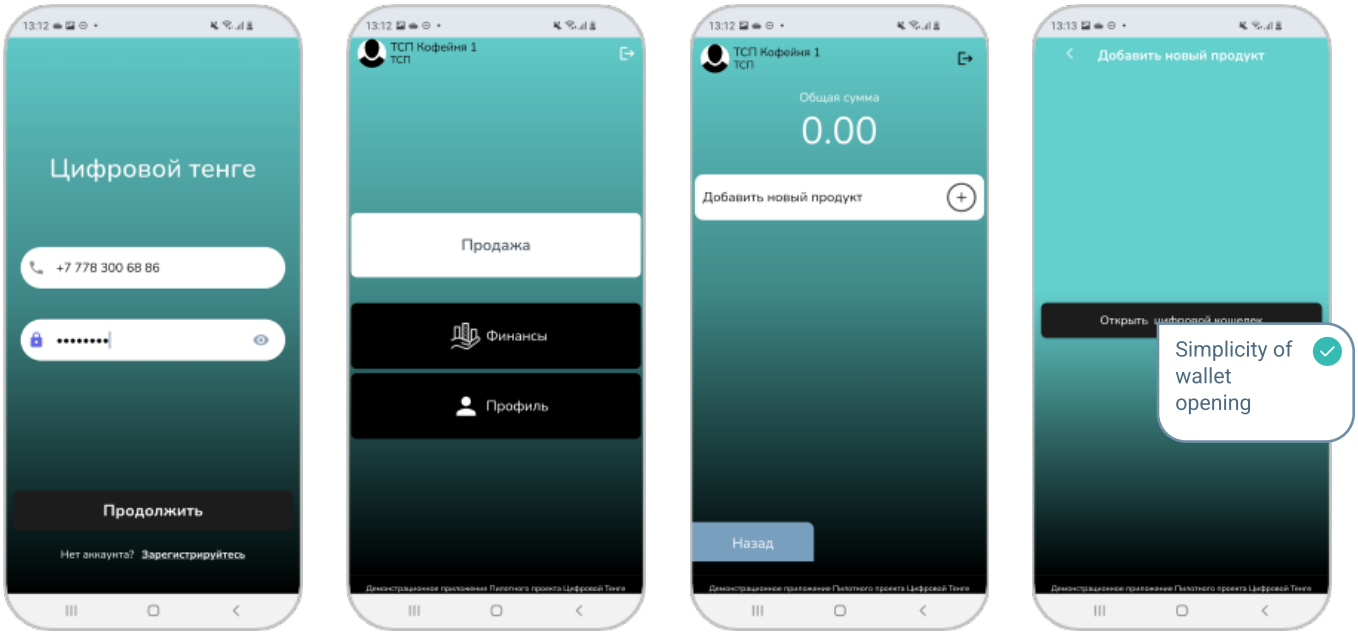
Opening wallets

01 → Merchant registers and logs in to the application

02 → Merchant clicks «Finance»

03 → Merchant clicks “Open new product”

04 → Merchant opens digital wallet



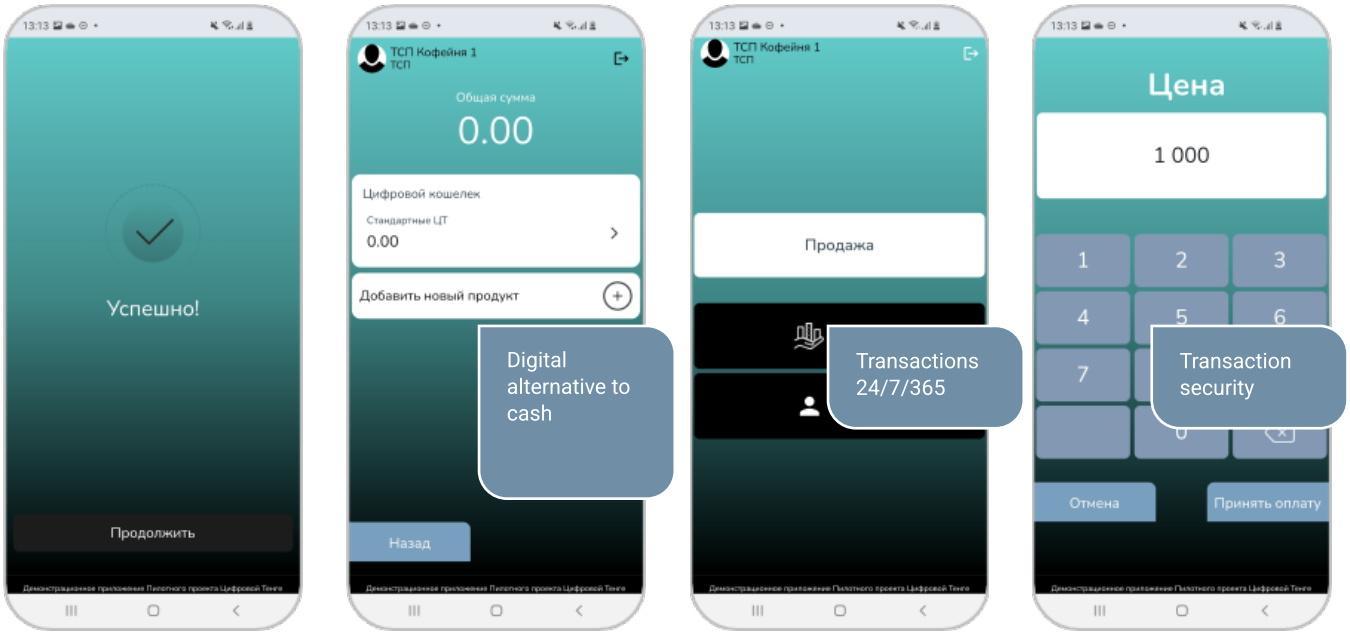
Selling

05 → Merchant sees that the wallet has been successfully opened

06 → Marchant sees his DT account details

07 → Merchant clicks «Sale»

08 → Merchant enters DT amount (standart or special DT)



Merchant MVP

Selling and checking transaction history

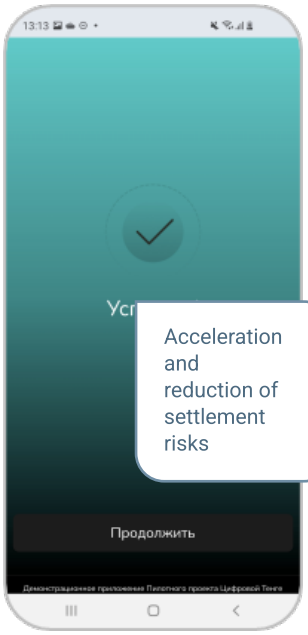
09 → Generating QR-code

10 → Merchant sees that the transaction has been successfully comleted

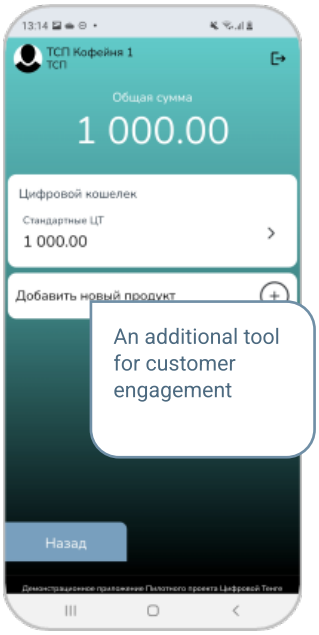
11 → Merchant sees updated balance of digital wallet

12 → Merchant checks the tranaction history

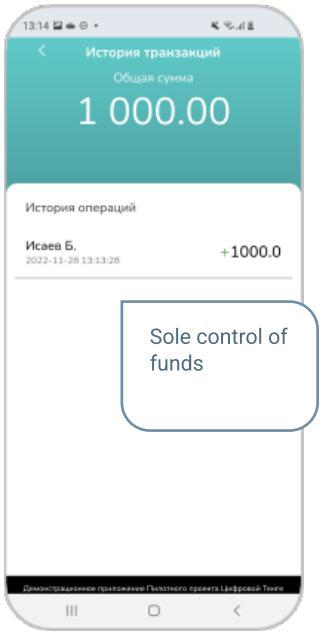
The usual method of payment by QR-code



Acceleration and reduction of settlement risks



An additional tool for customer engagement



Sole control of funds

Individual R&D

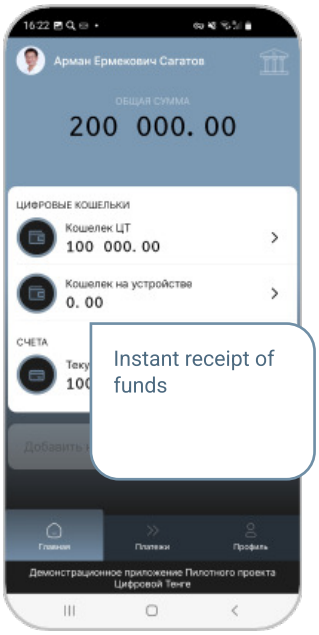
Открытие и пополнение кошелька

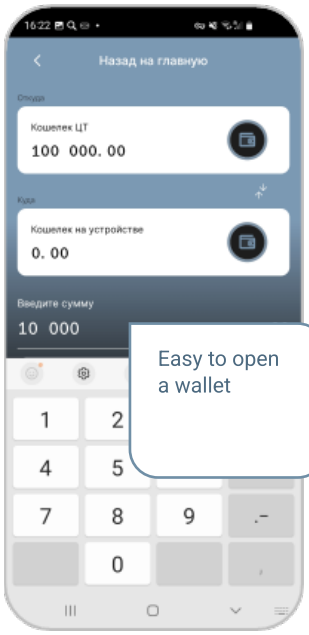
01 → Individual logs in to the application

02 → Individual opens digital wallets (online and offline)

03 → Individual sees his DT account details

04 → Individual clicks «Payments» to transfer money to local wallet





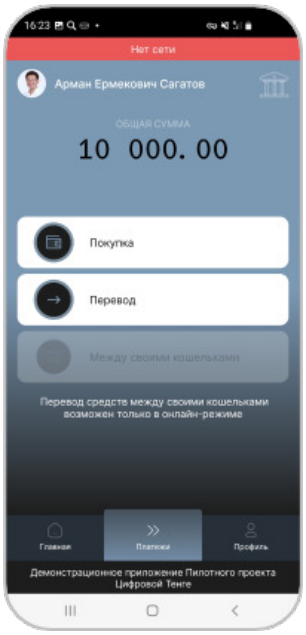
Offline transfer

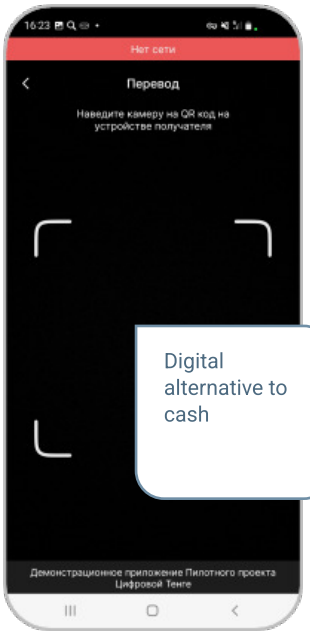
05 → Individual switches the device to the offline mode, clicks «Payments» and chooses «Transfer»

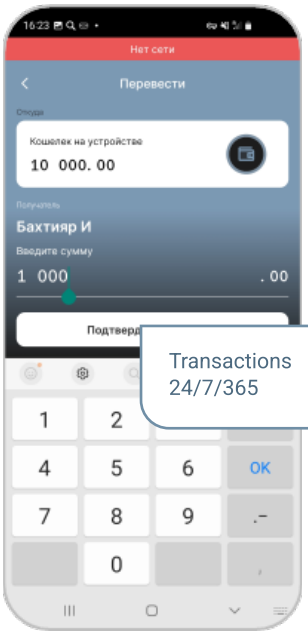
06 → Individual indicates that he will be the sender of the DT in the transaction and scans the QR-code of the DT receiver

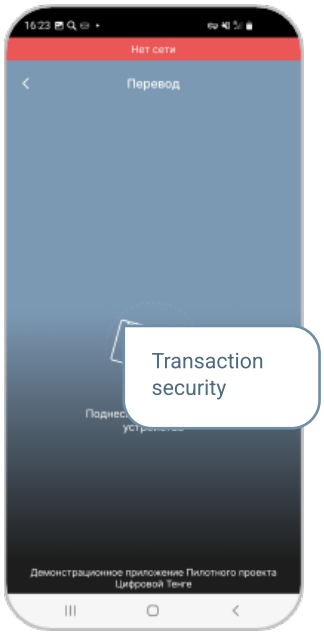
07 → Individual enters the DT amount to transfer, confirms transaction

08 → Individual brings the device closer to the device of another individual to make a transfer (NFC-transfer)









Individual R&D

Offline purchase, synchronization

09

Individual clicks «Payments» and chooses «Purchase»

10

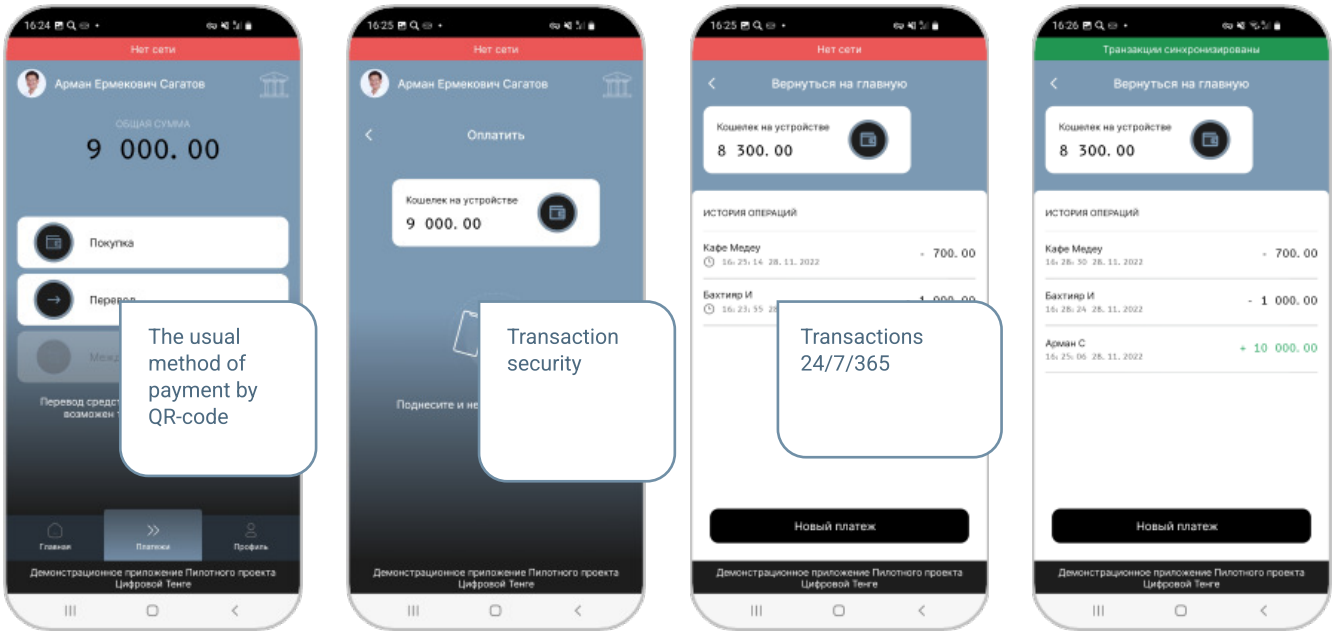
Individual brings the device closer to the merchant's device to make a purchase

11

Individual checks transaction history in offline mode

12

Individual connects to the Internet, transactions are synchronized



Merchant R&D

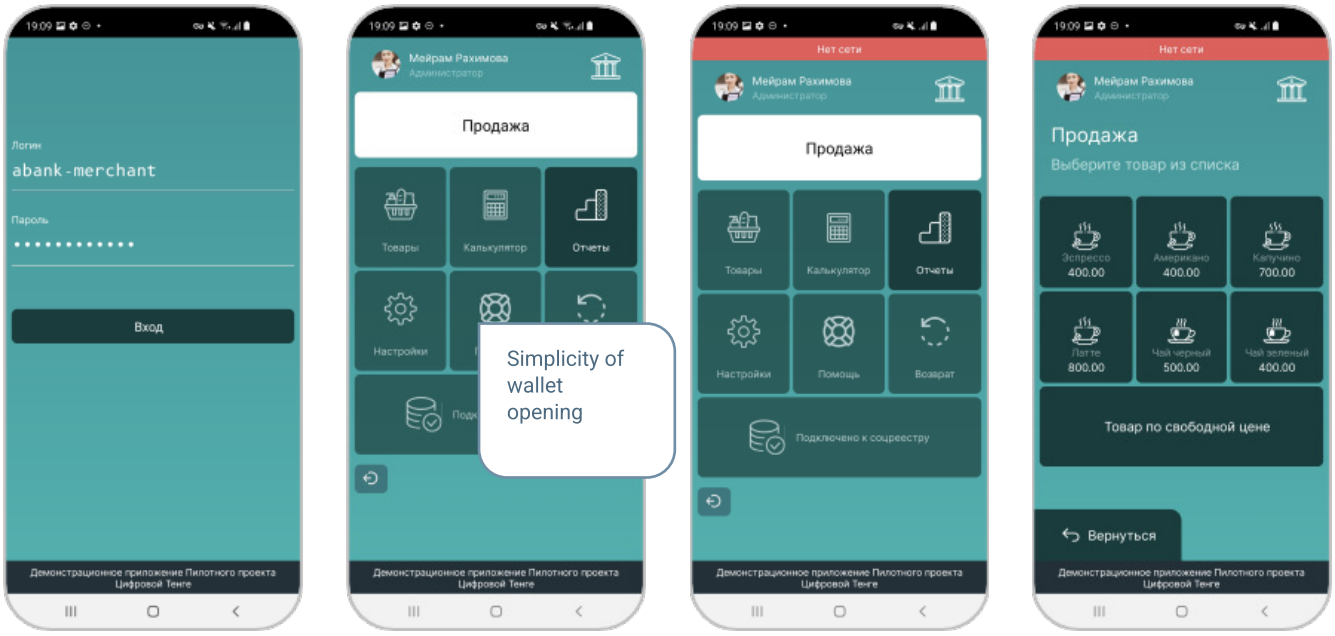
Opening wallets

01 → Merchant logs in to the application

02 → Wallets are opened automatically, merchant sees the main menu

03 → Merchant switches the device to the offline mode

04 → Merchant clicks «Sale»



Simplicity of wallet opening

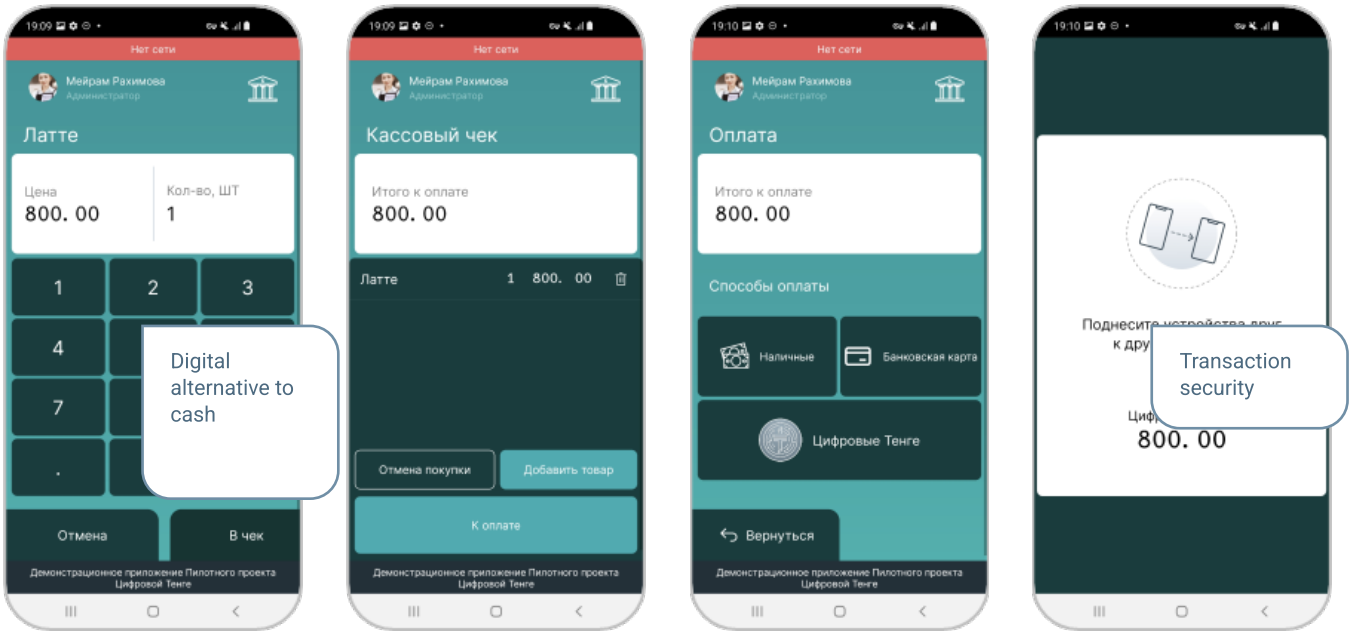
Purchase

05 → Merchant selects an item for sale or enters the amount of DT for payment

06 → Merchant clicks «Pay»

07 → Merchant chooses «Digital Tenge» as a payment method

08 → Merchant brings the device closer to the individual's device to make a purchase



Digital alternative to cash

Transaction security

Merchant R&D

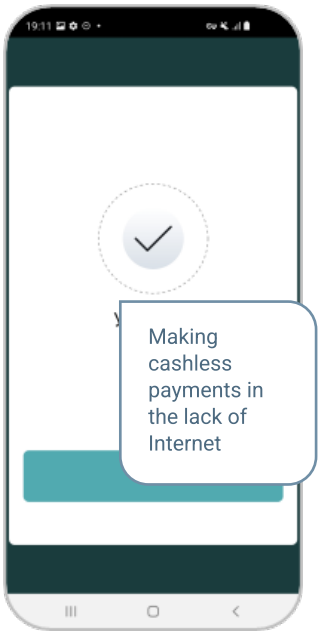
Purchase and checking transaction history

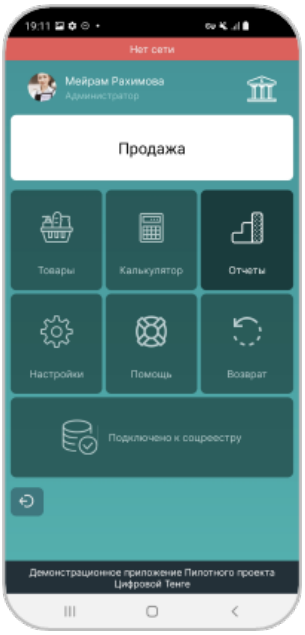
09 → Merchant sees that the transaction has been successfully comleted

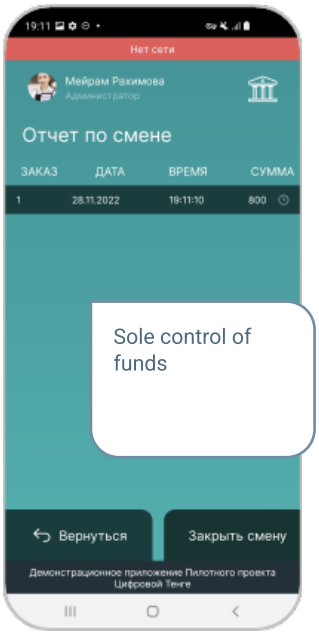
10 → Merchant goes to the menu, clicks «Reports»

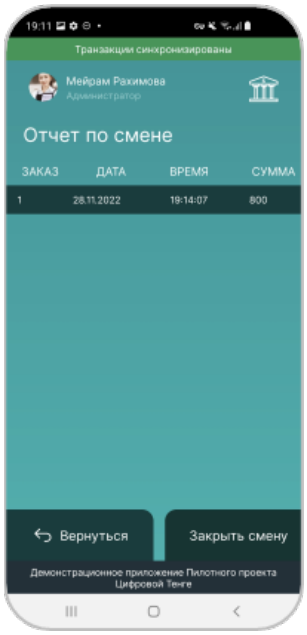
11 → Merchant checks transaction history in the offline mode

12 → Merchant connects to the Internet, transactions are synchronized









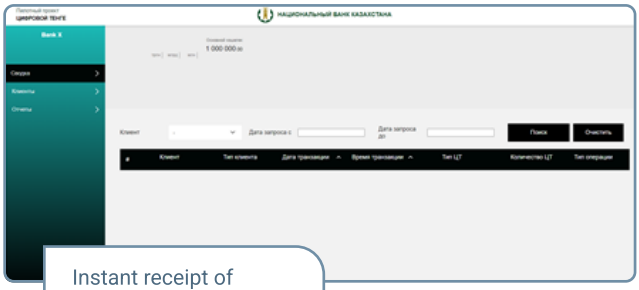
01 OPENING WALLETS AND DISTRIBUTION

FI/EP accesses the portal and opens a digital wallet

Simplicity of wallet opening

02 OPENING WALLETS AND DISTRIBUTION

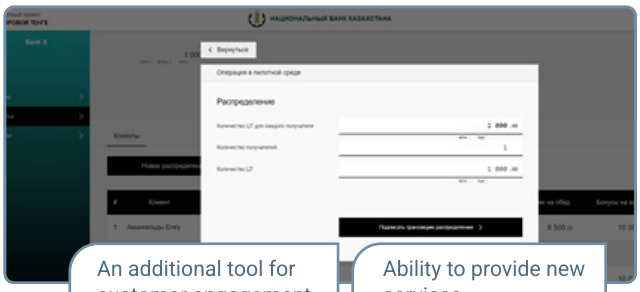
FI/EP sees DT in the wallet *(transfer from other forms of money / exchange for reserves will be implemented in the next phase of the project)*



Instant receipt of funds

03 MANAGING INDIVIDUAL'S WALLETS

FI/EP manages users' wallets, distributes DT to users, and verifies transactions

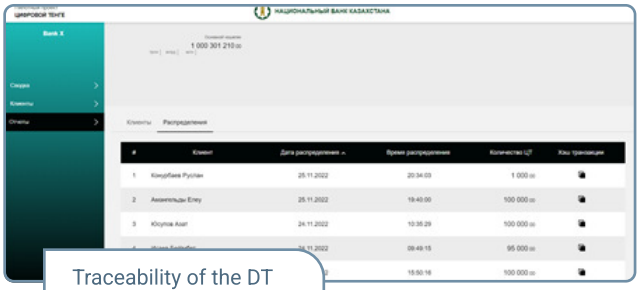


An additional tool for customer engagement

Ability to provide new services

04 MONITORING

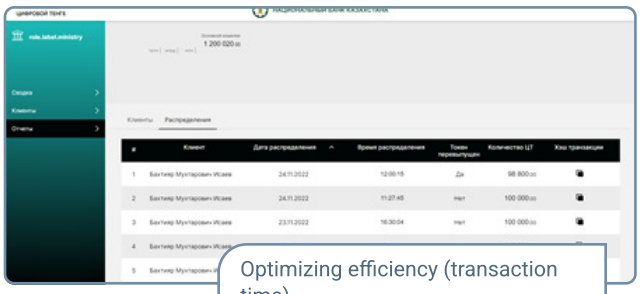
FI/EP monitors the use of DT by customers



Traceability of the DT

05 REISSUE

FI/EP makes a request to re-issue a token: redemption of a token with a long history and issuance of a new token



Optimizing efficiency (transaction time)

GA

01 OPENING WALLETS AND DISTRIBUTION

GA accesses the portal and opens a digital wallet

Simplicity of wallet opening

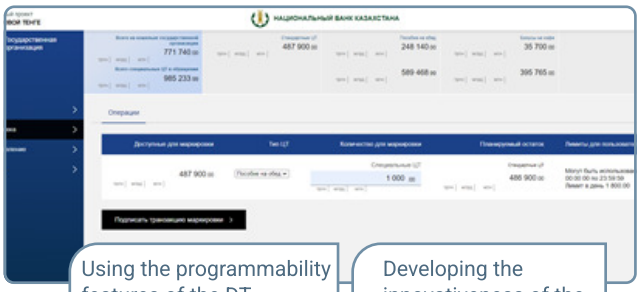
02 OPENING WALLETS AND DISTRIBUTION

GA sees the DT in the wallet *(transfer from other forms of money / exchange for reserves will be implemented in the next phase of the project)*

Instant receipt of funds

03 MARKING TOKENS

GA manages users' wallets, distributes the DT to users, and verifies transactions

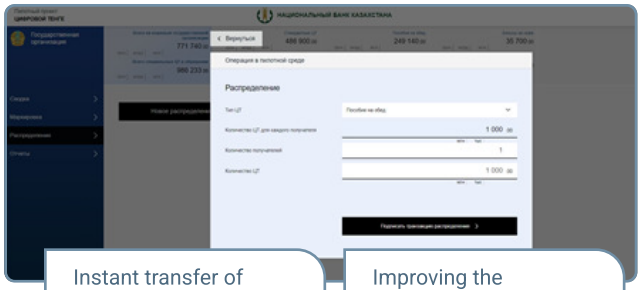


Using the programmability features of the DT

Developing the innovativeness of the financial sector

04 DISTRIBUTION OF SPECIAL DT

GA distributes the special DT to individuals

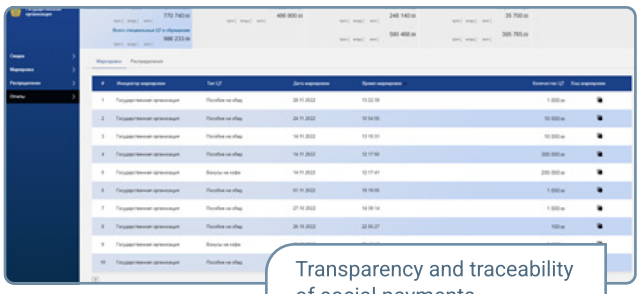


Instant transfer of funds (without intermediaries)

Improving the effectiveness of social benefits and inclusion

05 MONITORING

GA monitors the special DT (monitors the intended use)

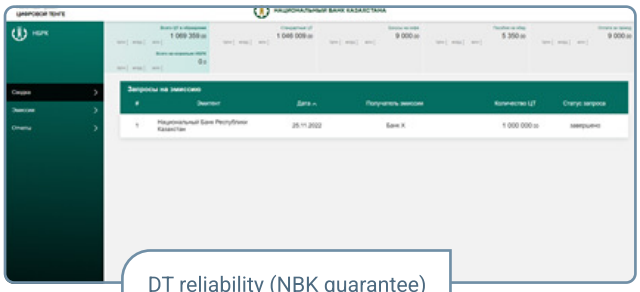


Transparency and traceability of social payments

NBK

01 ISSUANCE AND DISTRIBUTION OF FUNDS

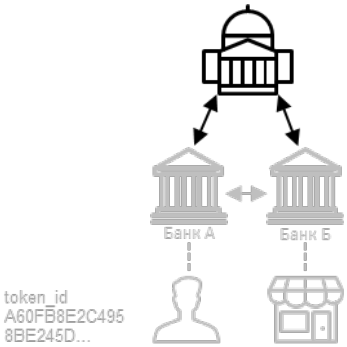
The NBK makes an issuance - issues new DT into circulation. The selected DT are distributed to the wallets of GA and FI/EP



DT reliability (NBK guarantee)

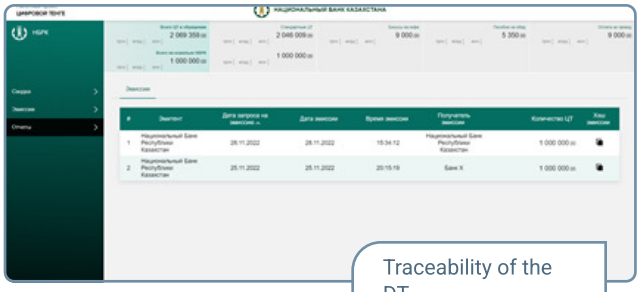
02 INTERACTION WITH INDIVIDUALS AND MERCHANTS

The NBK checks the uniqueness of the token involved in the transaction



03 MONITORING

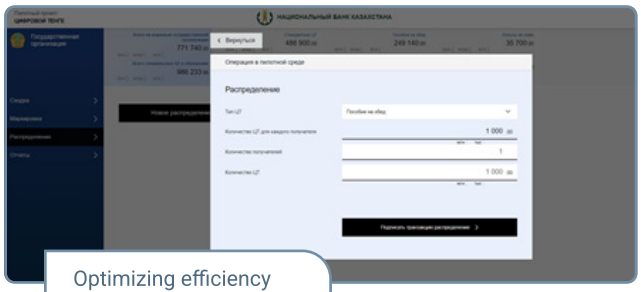
The NBK monitors issued DT



Traceability of the DT

04 REISSUE

The NBK reissues the DT: redemption of token with a long history and issuance of a new token without history

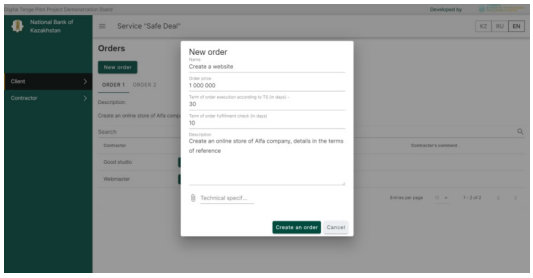


Optimizing efficiency (transaction time)

«Safe deal» scenario

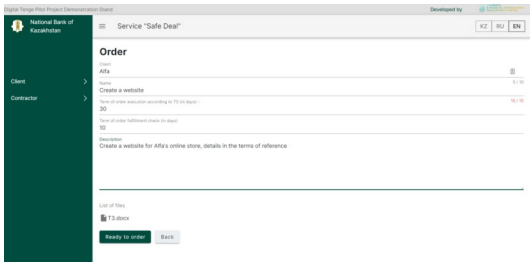
01 CREATING AN ORDER

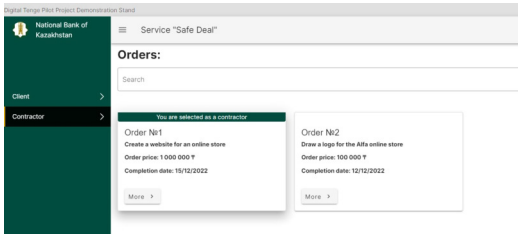
The contractor creates an order with specified amount and deadline. At the time of order creation, the amount is checked in the customer's DT purse and a smart contract is created



02 ORDER REQUISITION

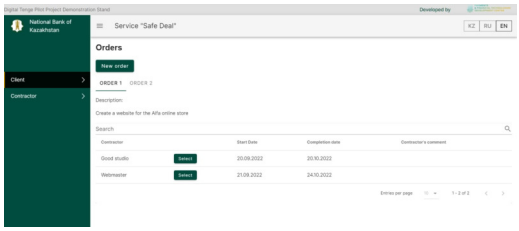
Potential contractors can see the list of orders, view order details and offer their services





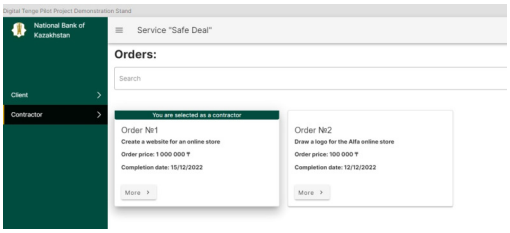
03 THE CLIENT CHOOSES THE CONTRACTOR

The customer chooses the contractor among those who responded to the order. Once the contractor is selected, the DTs on the customer's wallet will be reserved for the period of order completion. The contractor receives the notification and proceeds to the order execution



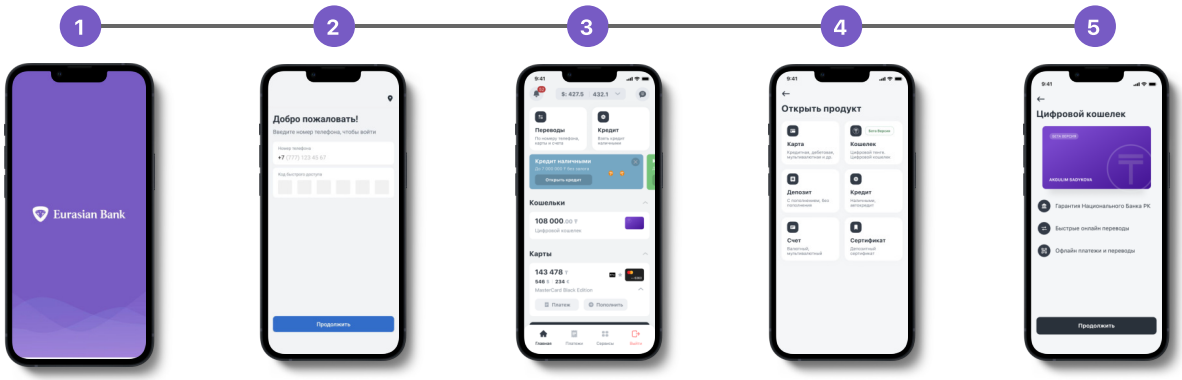
04 CLOSING THE DEAL

Каждый этап сделки фиксируется в смарт-контракте
The contractor completes the order and receives payment. After completing the order, the contractor notifies the customer. The customer confirms that the order is completed, and the funds are transferred to the performer's DT wallet. Each stage of the transaction is recorded in a smart contract

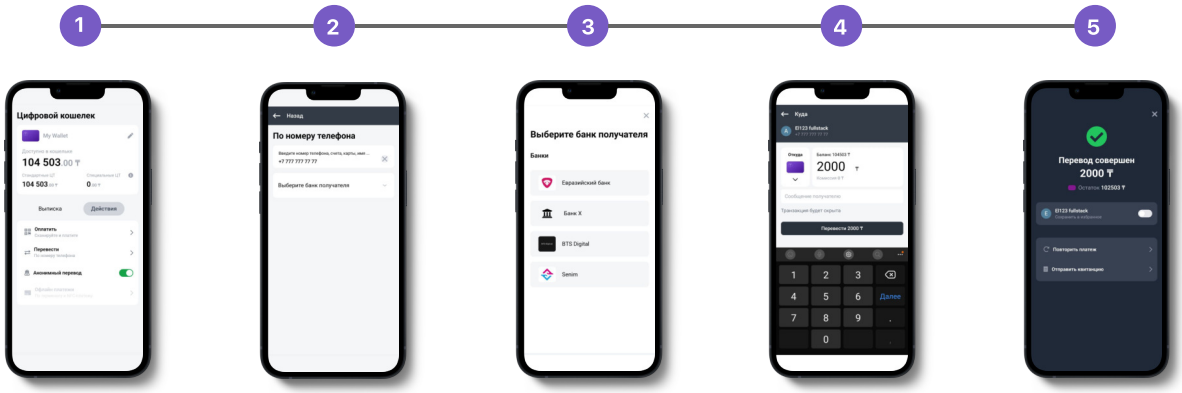


Eurasian bank's scenario

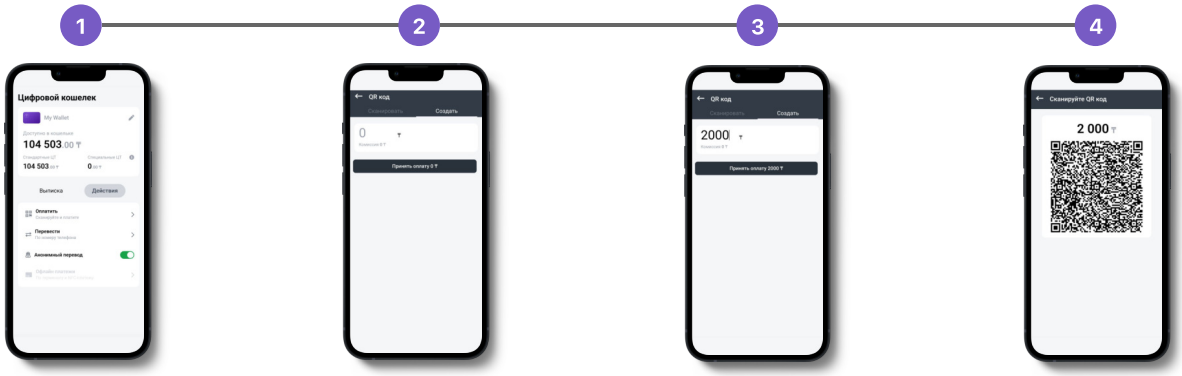
Opening wallets
(for individuals)



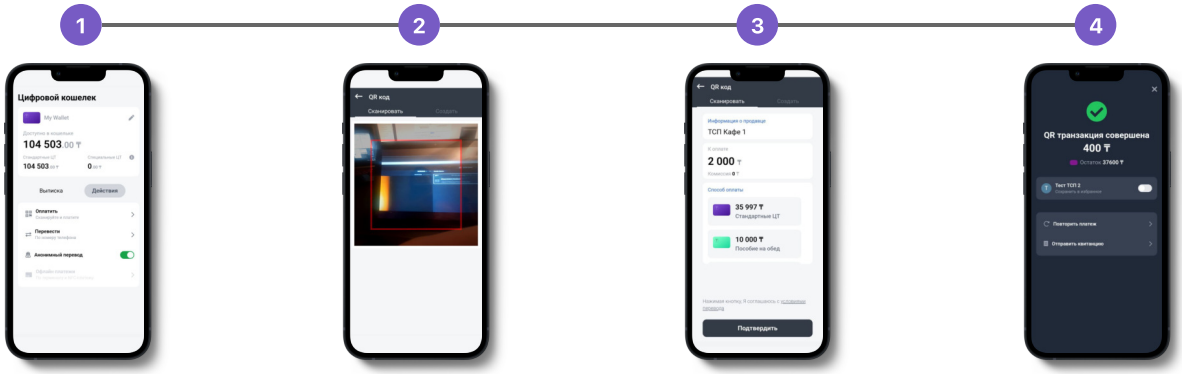
C2C transfer
(via mobile phone number)



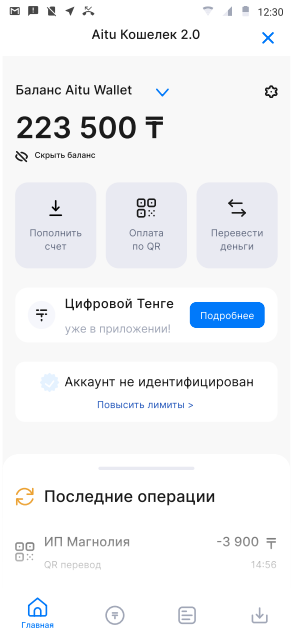
C2C transfer
(acceptance via QR-code)

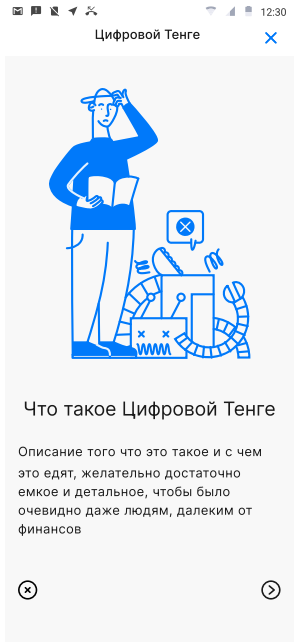


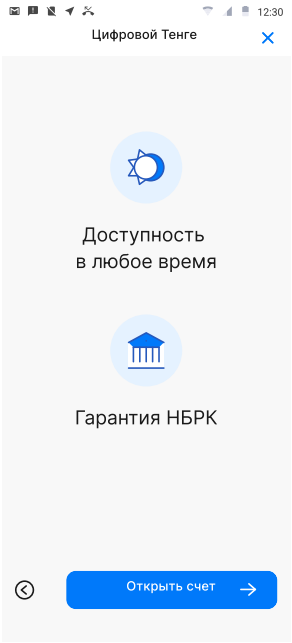
Purchase
(standard / special DT)

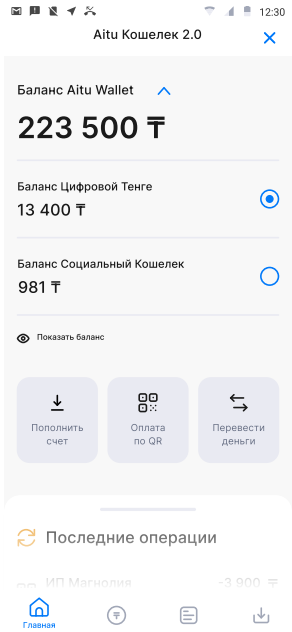


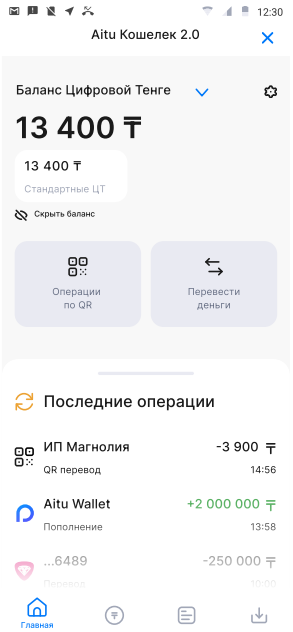
BTS’s scenario: Opening wallets





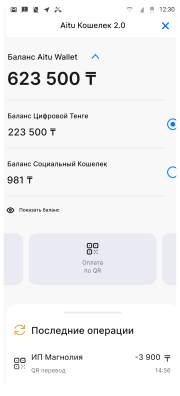






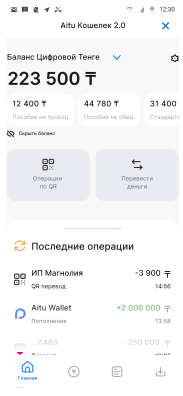
1. User logs in to Aitu Wallet, clicks on "Read more" about Digital Tenge
2. User reads brief information about the DT
3. User clicks "Open Account"
4. User sees a message that the wallet has been created and clicks "Main page"
5. User sees the DT’s blances on the main page and clicks on it
6. User sees the details of the Digital Wallet: types of the DT and active buttons: pay, transfer, transaction history

BTS's scenario: C2C transfer (via mobile phone number)



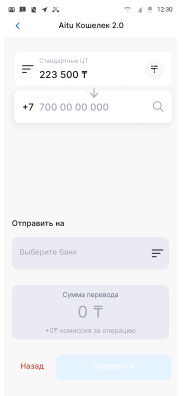
1

User-1 selects the balance of the Digital Tenge



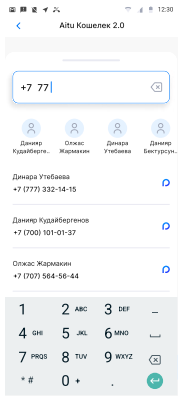
2

User-1 clicks on "Transfer Money"



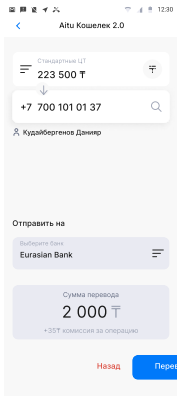
3

User-1 enters all necessary information for transfer



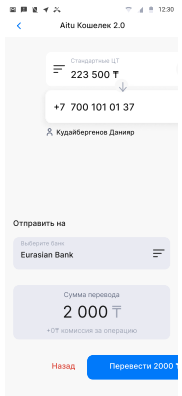
4

User has the ability to quickly add a phone number from the contact list



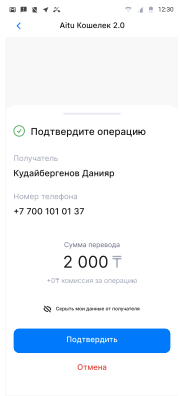
5

User selects a bank



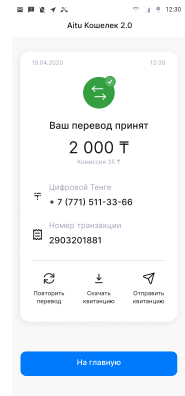
6

User-1 enters the number of the DT to transfer to User-2



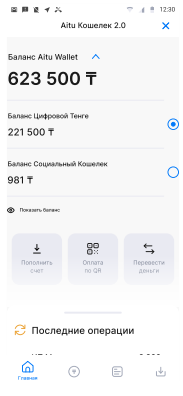
7

User-1 confirms transfer details



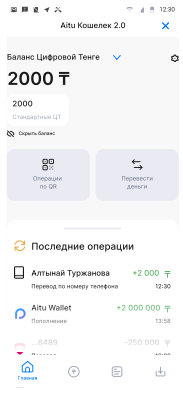
8

User-1 sees that the transaction was successfully completed. It is possible to return to the main page.



9

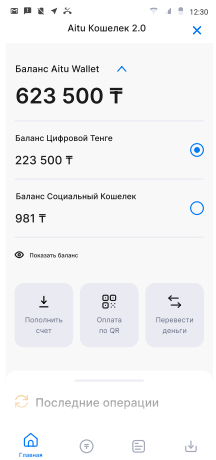
User sees the updated balance of the DT in Aitu Wallet



10

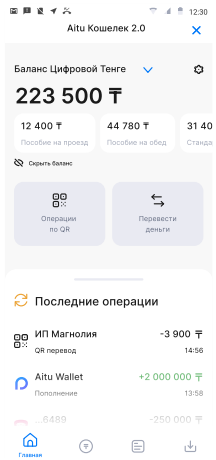
User-2 sees the updated number of DT. The transfer details can be checked in the transaction history.

BTS’s scenario: Purchase (Standard DT)



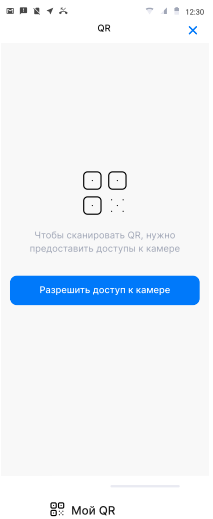
1

User logs in to the Aitu Wallet app



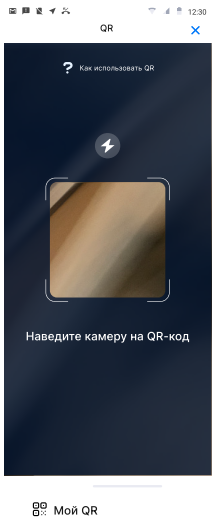
2

User selects “Digital Tenge balance” and clicks "QR Transactions"



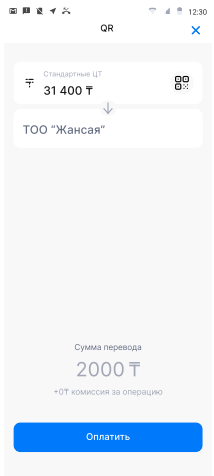
3

User agrees to use the phone camera



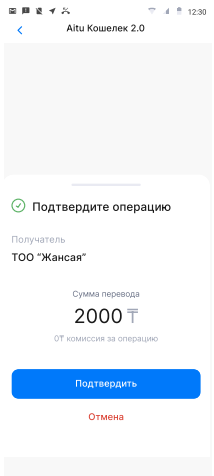
4

User scans QR-code on a cashier's device



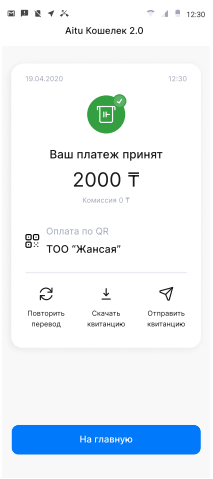
5

User selects the method of payment by the standard DT. The recipient and the amount of money are known and static, clicks on "Pay"



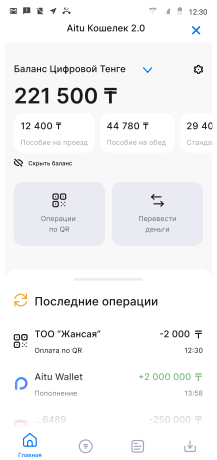
6

User-1 confirms payment details



7

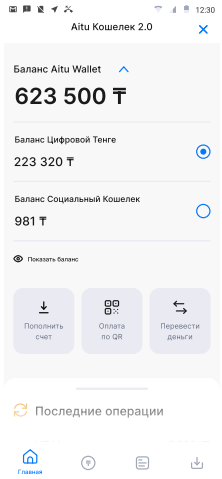
User sees payment confirmation and goes to the main page

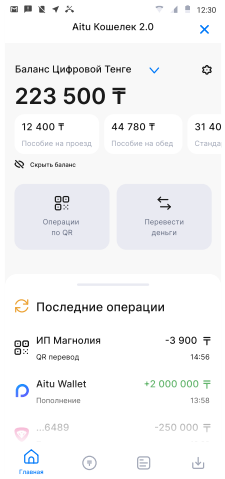


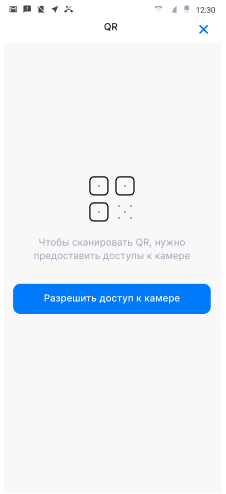
8

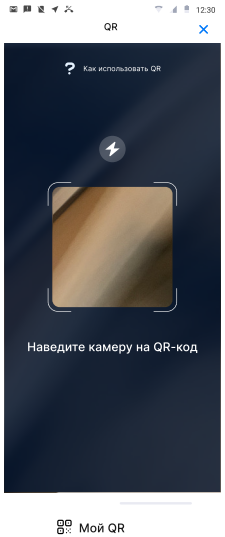
User sees updated balance of the DT in the Aitu Wallet

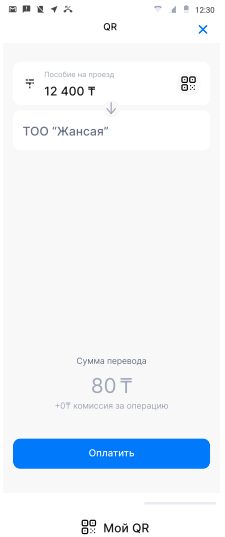
BTS’s scenario: Purchase (Special DT - Fare payment)

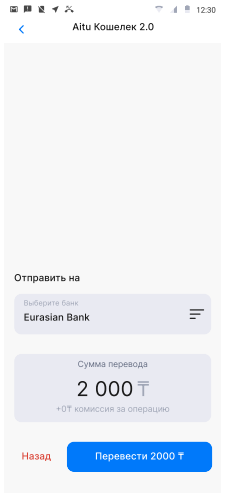


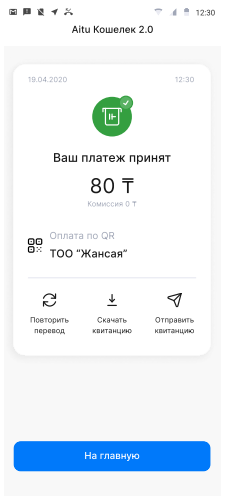


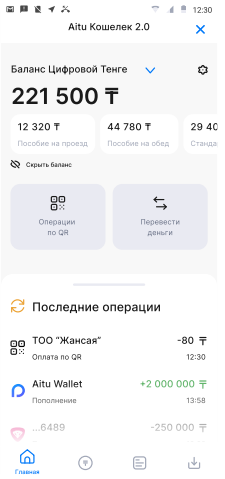












1. User logs in to the Aitu Wallet app
2. User selects “Digital Tenge balance” and clicks "QR Transactions"
3. User agrees to use the phone camera
4. User scans QR on a device to pay with a card in the bus
5. User selects the method of payment by the special DT: fare payment. The recipient and the amount of money are known and static, clicks on "Pay"
6. User-1 confirms payment details
7. User sees payment confirmation and goes to the main page
8. User sees updated balance of the DT in the Aitu Wallet

Analysis of available mechanisms to reduce the risk of double-spending, money laundering, and terrorist financing

The pilot project implementation is based on the principles of the UTXO model where a transaction supports the transfer of ownership of a token from one user to another. Currently, offline transactions use tokens from offline wallets which during their depositing on the device are signed by the FIs/EPs, guaranteeing their authenticity.

Without the Internet connection, the receiver of the payment can verify the authenticity of the funds received by checking the history of the token transmitted with it, up to the bank's guaranteed signature. When one or both participants of the transaction go online, the entire token history from offline mode and all payment orders are transferred to the participants' FIs/EPs nodes and the notary node for finalizing transactions..

Validation at the notary node level guarantees verification that the token has not been used before, thus minimizing the risk of double spending. The revealed fact of double spending in the offline framework should be transferred to law enforcement agencies for investigation and application of measures defined by law (equivalent to counterfeiting cash). The legislation matters and legal procedures were not worked out during the pilot phase. When choosing a technical solution for the implementation of the "last mile" in the target DT platform, depending on the chosen solution, it is necessary to work out mechanisms for controlling double spending at the device level.

Transaction verification at the FIs/EPs level guarantees valid transactions. Even with the implementation of user-customizable anonymity, FIs/EPs may continue to conduct KYC checks on their customers or, if necessary, compare transaction data with real customers.

To control the risk of money laundering and terrorist financing, the programmability of the token (at the level of its structure) and reconciliation of ownership rights with special block lists of owners could be used. A special block list is maintained by the NBK in the platform. The practical research of AML/CFT was not the focus of the R&D study of offline payments. However, risk within the DT platform needs to be considered. Risk considerations were incorporated into the DT platform architecture, and the possibility of implementing risk considerations to prevent future money laundering and terrorist financing activities has been analytically confirmed.

Analysis of the possible technologies for conducting a chain of offline transactions based on user-friendliness

Within the study, a comparative analysis was conducted to determine the **potential application of different data transfer technologies over mobile devices** based on their user-friendliness.

For the R&D study, a combination of QR-code and NFC was used to provide the necessary functionality and convenience for the user, as well as to focus on the main goals of the current stage, reusing the experience of PoC and MVP. In the target solution, further research on alternative technologies to increase the level of UI/UX is recommended (contactless transfer in a minimum number of customer actions/in a minimum time).

Analysis of the possible chain length of offline transactions

Within the study, the analysis of factors affecting the acceptable length of the chains of offline transactions was conducted. As the number of offline transactions grows, the volume of transmitted information increases. This ultimately affects the time of its execution.

The assessment of the acceptable volume of the offline transaction token from the transaction history was conducted based on:

- Token structure
- Required data for offline transactions
- Patterns of increasing offline token history
- Transfer of transaction history as proof of the origin of the token from the deposit point
- Technological limitations
- NFC technology limit in data transfer rate
- Non-functional requirements
- Transaction time

According to the results of the practical R&D experiments and considering the transaction time requirement of 5 seconds, the acceptable token history length was 6-7 transactions, which is equivalent to 6-7 transactions conducted offline from one user's device, or 6-7 transactions conducted sequentially between different user devices.

The potential token history length could be higher by increasing the data transfer rate supported by the selected data transfer technology to mobile devices, as well as by exploring compression mechanisms for transmitted data

Technical requirements and limitations on users' devices for offline transactions

To ensure stable operation in the offline mode, it was decided that device models with Android OS versions (12 and higher) with NFC and host card emulation support were used. To enable offline mode (storing transaction history and signature verification data), it would be necessary to consider the required amount of free memory available on the device. The results suggested that the device would need to have an allowable length of token history, so the device must have a memory that satisfies at least 5.5-6 kilobytes of storage. This is an insignificant amount of data compared to the size of the application itself.

Analysis of the need for functional limits applicable to an individual offline wallet

According to the results of the study, it was concluded that the introduction of centralized limitations (a limit on the amount for the deposit, on the maximum transaction amount, on the maximum number of transactions, etc.) is technically implementable, even if it narrows the user's capabilities, compared to its cash counterpart. The security of offline payments also does not increase with such functional limitations. It is recommended at the level of the banking application in the target solution to provide customers with the opportunity to set their limits on wallets (for example, a limit on the amount of spending per period).

The influence of offline transactions on node performance

It is expected that every offline transaction may generate an unvalidated payment order on each transaction participant's device. Additionally, the following participants in the DT exchange chain will receive a transaction history.

As a result, when going online, one payment order will get to the processing nodes as many times as it participated in transactions. The node will execute each payment order only once, the rest will be rejected. The higher the number of participants in offline mode and the more transactions they carry out, the more "duplicates" of payment orders will get to the nodes for processing. To ensure the enablement of the non-functional requirements of the platform, it is necessary to consider additional requirements for the infrastructure. This means considering the load from offline transactions, as well as effective mechanisms for controlling duplicates.

Preparation for the pilot project

The technological features of the Corda platform that affect its performance were identified when preparing the system for piloting. Comparable results of payment systems with similar characteristics were used as reference values for performance during the tests.

Resource usage

Non-optimal resource usage can lead to delays in transaction processing or even to a system crash. Tests were made with random access memory and central processor unit load measurements on bank and notary nodes. The results showed that the infrastructure resources are used optimally

Containerization

Containerization is designed to optimize deployment and CI/CD. Transactions with and without containerization of nodes were measured in two test scenarios; tests with the use of containers showed improved performance by optimizing the use and management of resources. For the pilot project, it was decided to use containerization.

In-memory database

Alternative DB solutions can optimize backup time with faster processing. PostgreSQL, the default database used in the Corda Community edition, and an in-memory database on a pilot load were measured.

The measurement results showed that in-memory database placement gives an insignificant improvement in response time and error rate. At the same time, there are risks such as unreliability for the production environment (when the database consumes all allocated memory, it stops processing; in the case of server downtime, the database is erased). In this case, it is necessary to implement additional backup mechanisms, but they may also affect performance. Also, the default PostgreSQL database is not designed to be used in memory (Redis DB, Apache Ignite, and others are commonly used, but they are not the default Corda database). Default database was utilized for the pilot project.

Comparison of processing times for diverse types of transactions

The duration of transaction processing depends on the complexity of the business logic embedded in it. Custom transactions (transfers and purchases) are among the most multi-component ones in the system, their flow consists of many exchanges between FI/EP nodes, notary node, as well as cryptographic calculations (sum hiding, configurable anonymity, transaction signatures).

Comparative measurements of processing times for user transactions (purchases and transfers) and the simplest transaction in the system (issuance transactions) showed that the system withstands a larger load and shows better response times for simple transactions than for complex ones. The maximum load on simple transactions was several times greater than on simple transactions while maintaining the target response time.

Transaction profiling

Time measurements were taken for processing each step in the transaction process.

The results showed that there is a **queue on the nodes due to the single thread processing limitation in Corda Community Edition** and Corda's built-in flow processing mechanisms. Also, during the processing of each transaction, the node continually creates its backup for disaster recovery.

Several large queries to NODE_CHECKPOINTS tables (insert, update, delete) account for over 75% of all data processed. Corda's technical documentation notes this process as creating a "bottleneck" for performance [1]:

These tables have the heaviest read-write load, especially in NODE_CHECKPOINTS and NODE_CHECKPOINT_BLOBS. Depending on the flow used and the load on the node, operations on this table will be a major bottleneck in node performance.

Multithreading

Multiple threads for request processing allow more operations in parallel mode in case there is spare capacity. The Corda Community version has a vendor-defined limitation of using only one thread (single-thread only). Corda Enterprise features the ability to configure multi-threading on nodes using two parameters (rpcThreadPoolSize, flowThreadPoolSize); the vendor recommends these parameter values be set according to infrastructure resources (depending on the number of logical cores). We measured processing speed and error rate in test scenarios for several configurations: Corda Community (1 thread) and Corda Enterprise (multiple threads), pilot load, and error-free load.

The results of the measurements showed that multithreading significantly improves performance indicators within the limits of the conducted tests: it allows increasing throughput several times and reduces average latency, reducing the percentage of errors in queries to an insignificant level.

Conclusions on the results of performance testing in preparation for the pilot project

The developed DT platform can run on both Corda Community Edition and Corda Enterprise Edition. Based on the results and studies of load testing it is revealed that now **the platform covers the throughput requirements** of the pilot project, but to achieve performance in the industrial-scale-environment several additional performance optimization tasks need to be implemented when developing the solution, both based on CCE and CEE.

Details of the possible scope of work, as well as the risks and costs associated with the choice of a particular scenario of platform development, are presented in Table below.

Corda Version	Corda Community	Corda Enterprise
Potential (non-exhaustive) scope of work	• Refinements in source code to implement multithreading and a customizable messaging mechanism between nodes • Analysis of key factors affecting performance and fine-tuning to achieve the performance of the industrial DT platform	Analysis of key factors affecting performance and fine-tuning to achieve the performance of an industrial DT platform
Benefits	Full control over the development, including intellectual property rights	• Vendor support for the platform • Migration to Corda 5 (after the official version release) will expand performance optimization capabilities (modular code, use of Kafka for messages, integration with Kubernetes)
Risks and costs	• Significant labor costs to rework the source code • Creating a branching off from the original version - integration of add-ons of Corda versions/migration to a higher version becomes nearly impossible • Full functional and load testing of compatibility of add-ons with Corda platform core functionality • Lack of vendor support for the platform	• The cost of the license • Higher vendor dependency

The developed DT platform can work on both Corda Community Edition and Corda Enterprise Edition . Load testing results show that the platform covers current Pilot throughput requirements, but to achieve performance on a production level, it is necessary to implement a few additional performance optimization solutions during development, regardless of Corda edition choice.

At the moment, the biggest impact on the performance of the solution comes from:

- The existence of standard Corda backup processes, which account for more than 75% of the data in processing each transaction;
- The presence/absence of multi-threaded transaction processing;
- Single-threaded processing when checking token transaction history.

Further optimization recommendations are described in the technology section of the internal report:

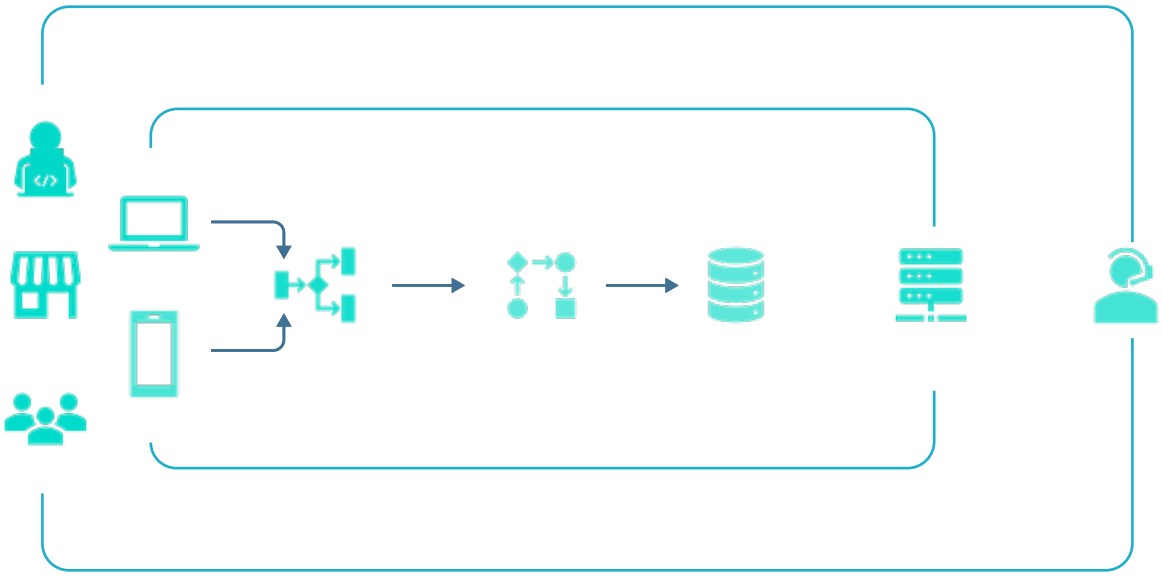
The target DT platform must withstand high loads due to its use at the level of the entire population of Kazakhstan, respectively, an important preparatory stage for bringing the solution into production should be extensive load and stress testing and performance optimization of the platform to maintain the necessary SLA.

It should be noted that a noticeable performance improvement can be achieved only through the cumulative effect of optimization on all layers of the solution.

Because front-end solutions and the mid-layer are in the loop of external participants, it is important to set up collaboration and synchronization on results between all platform participants, as well as to set uniform performance metrics to track results.

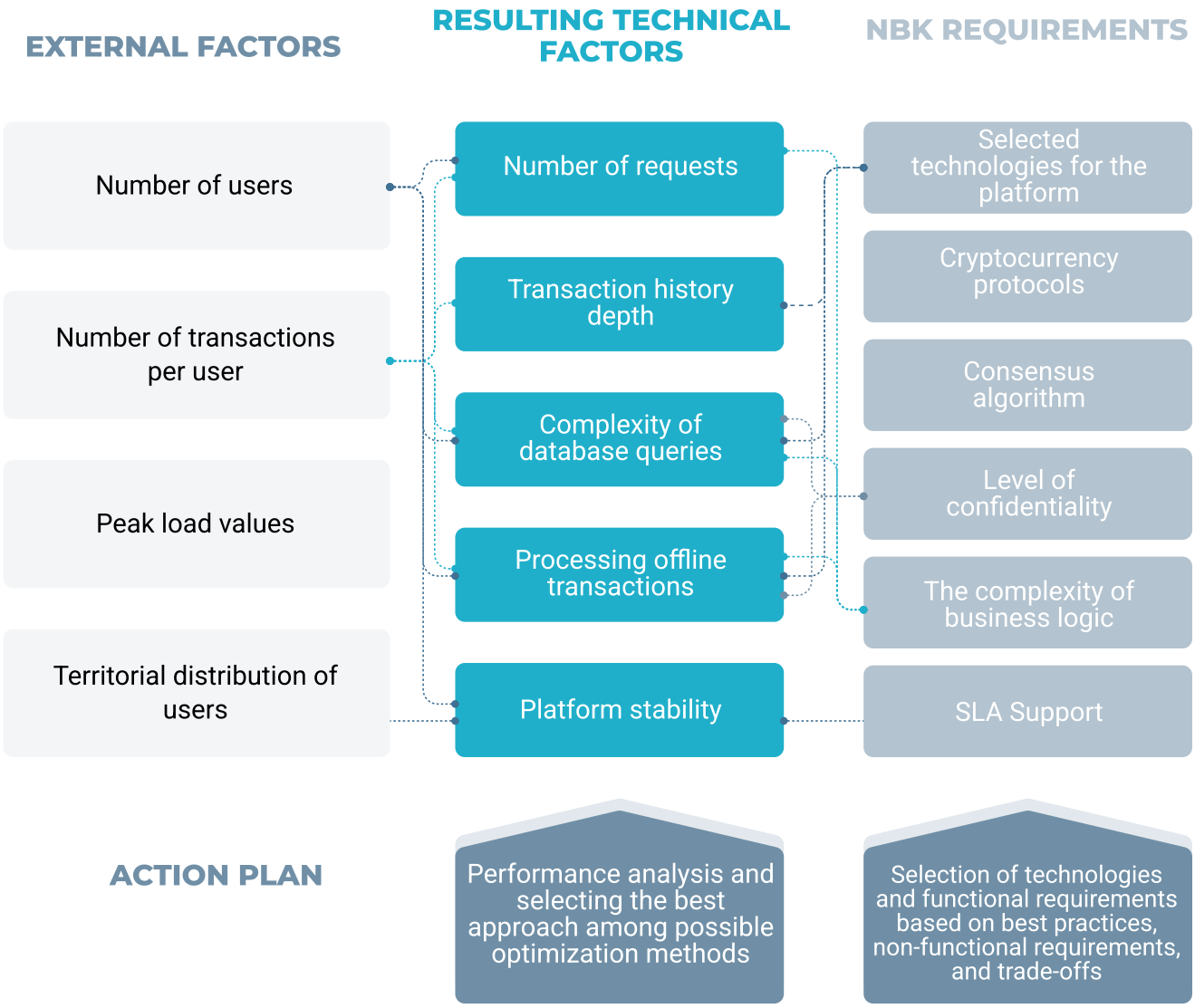
Such metrics can be:

- number of transactions processed per second by the DT solution (the DT platform + front-end application);
- transaction processing time on the side of the DT platform;
- the transaction time for a user (considering the time for data processing and rendering on the front-end application).



FRONT-END	Focus on user experience (customers, employees) based on the overall performance of front-end applications and the platform
MIDDLE LAYER	Individual optimization of integration between front-end and back-end **specific to each front-end application**
BACK-END	**A "Test & try"** approach to platform customization to balance tradeoffs in functional and non-functional requirements
DATA BASE	Setting up an optimal database configuration **combined with backend optimization**
INFRASTRUCTURE	Providing **platform flexibility** to accommodate peak loads, seasonal changes and country geography
SUPPORT	**Basic foundations** for overall platform availability, stability, operability and reliability

The performance of the entire DT solution (DT platform and front-end applications) depends on various external factors and inherent business requirements and technological choices. System requirements and technical factors should be the focus of the analysis and performance-tuning work.



Depending on the results of the analysis of the prevailing factors, different methods of performance optimization can be applied, and the specific recommendations within each method differ.

	FACTORS AFFECTING PERFORMANCE	POSSIBLE OPTIMIZATION METHODS (prioritized by simplicity of implementation and efficiency)
NBK REQUIREMENTS	Selected technologies for the platform (including last mile solutions)	• Permanent monitoring of mature/industrial solutions • Selecting solutions based on best practices and balancing functional requirements and NFT test results
	Cryptocurrency protocols	
	Consensus algorithm	
	Level of privacy, amount of hidden data	• Permanent optimization of user code and performance tuning depending on changing requirements • Deciding on key tradeoffs (functional complexity vs performance and stability vs security)
	Complexity of platform business logic (e.g., smart contracts, programmability, number of nodes involved in a transaction, transaction confirmation logic, etc.)	
	SLA support	• Definition of SLA depending on the criticality of functionality • Platform reliability management
RESULTING TECHNICAL FACTORS	Number of requests	• Load balancer configuration • DT platform code optimization (multi-threading, resource utilization, data mining) • Configuration of on- and off-ledger storage • Automatic vertical scaling • Client application optimization (reduce number of requests, pagination, skeleton load) • Event streaming • Caching (both types) • Horizontal scaling of notaries and member nodes • Backend for Front-end implementation • Using HTTP2 protocol
	Transaction history depth	• Optimizing platform code (reducing transaction chains)
	Complexity of database queries	• Database optimization (indexing, connection pooling configuration, pre-calculated data marts, clustering)
	Processing offline transactions	• Optimizing platform code (data search)
	Platform stability	• Platform reliability management • Automatic vertical scaling • Horizontal scaling of notaries and member nodes • Highly available clusters supported by geographically distributed data centers

Principle	Strategic forks	Technological solutions	PoC design	MVP and R&D Design	Potential vision
Approach to Privacy	**Identity management:** • Anonymity vs pseudo-anonymity from the NBK and FI/EP • Ability to use anonymous wallets	**Integration with national universal services:** centralized eKYC vs KYC is conducted independently by each FI/EP and integrated with eID	**Primary anonymity:** Node-level address hiding, which limited the functionality to have the client sign a transaction using a one-time stealth address. The amount written in the token is hidden (homomorphic cryptographic commitment)	**Additional functionality:** Transaction-level anonymity with stealth address, functionality configurable from the user side. The amount written in the token is hidden (homomorphic cryptographic commitment). A certifying Kernel signature is also generated	**Anonymity:** Using confidential computing in a trusted code execution environment to keep user keys private
Traceability of transaction history	• **Traceability:** full anonymity (no access to data and transaction history) vs limited, traceability by NBK or regulator upon request vs full traceability by NBK, regulator, and FI/EP **Account and wallet management:** token-based model vs account-based model on top of the token-based model (with additional account controls and programmability)	**Security:** Data access is restricted at the DT platform level vs restricted at the level of secure spaces (enclaves)	**Traceability by nodes:** • Token transaction history from issuance • Transaction history is stored in FI/EP node storage	**Additional functionality:** Transaction history is "truncated" when the token is reissued, with saving to the NBK node storage	**Limited traceability on request:** Access to data needed for monitoring, investigations, AML/CFT on-demand with a special key

Principle	Strategic forks	Technological solutions	PoC design	MVP and R&D Design	Potential vision
User-friendliness of the DT	**The DT's features:** properties of cash and tokenization of ownership (incl. in case of loss of connectivity - offline) vs e-money **Account and wallet management:** • Wallet model selection • Using all tokens offline vs separate offline wallets • Limitations for offline use (time interval, number of transactions, amount, ...)	**Security:** Level of protection against unauthorized entry and offline hacking (algorithmic vs hardware- or software-based security or its combination)	**A token-based model with storage on the user's device** • One user = one device • Maximum one offline transaction before synchronization with an online node	**A token-based model with storage on the user's device** • One user = one device • Experiments with offline transaction chains	**Hybrid model** • Separate wallets - with online-only support and offline transactions • Separate offline wallets for different user devices • Using a secure code execution environment for data storage and code execution
The possibility of restoring DT	**Wallet management:** • Wallet model selection • Who bears the risk of financial institution failure (the NBK using reportable data to reissue user wallet vs users are fully responsible for their wallets in FI/EP) • Using all tokens offline (difficult to recover legally) vs individual offline wallets (online wallet can be fully recovered) • Who bears the financial and legal risks and liabilities of wallet recovery (FI/EP (restrictions on online or also offline wallet) vs users (full ownership and responsibility))	**Security and privacy:** centralized reporting at the NBK node level vs reporting in a secure space with on-demand access to NBK	**A model without reporting data** • Single online and offline wallet • Recovery is legally complex and must be further elaborated • User risks all the DT intended for offline use if the device is lost	**Model without reporting data** • Separate wallets - 1) with only online mode support, 2) with offline transactions option • User runs the risk of losing DT from the offline wallet, in case of loss of the device (no recovery procedure)	**A mixed model with reporting data** • Separate wallets - 1) with only online mode support, 2) with offline transactions • Online wallet can be restored, user can request FI/EP to block online wallet (in case of loss, fraud, etc.) • Offline wallet can be restored if regulatory aspects are worked out • Regular reporting and backups of user wallets to the NBK node repository to eliminate the risk of FI/EP error or misconduct

Principle	Strategic forks	Technological solutions	PoC design	MVP and R&D Design	Potential vision
Accessibility to participants and operability	**The role of market participants:** • The range of market participants and the extent of their participation • Centralized control by the NBK vs distributed responsibility within the NBK restrictions and templates (the NBK determines participant access levels) • Wallet management: token-based model vs account-based model over the token-based model	**Implementation of programmability:** network fully controlled by the NBK vs limited access for some participants (network-level access, release-level access...)	-	In the first experiments in the R&D sandbox - participants had the opportunity to develop scenarios and test hypotheses	• Centralized QA and CI/CD for smart contracts are provided by NBK • Account properties can be added on top of the token-based model to provide access to a wider range of participants

Principle	Strategic forks	Technological solutions	PoC design	MVP and R&D Design	Potential vision
DT security	**Partnerships:** Choosing an offline approach and appropriate partners (OS providers, smart devices, ...)	**Security:** • Algorithmic vs hardware- or software-based security vs a combination of the two • Approaches to online and offline security	**Algorithmic security** Cryptographic primitives (based on Edwards curves)	**Algorithmic security** New protocol for offline transactions (to implement offline chains)	**A combination of security approaches** • **Online:** confidential computing and use of cryptographic libraries issued by GA in Kazakhstan • **Offline:** partnering with OS vendors and using a trusted execution environment on devices to store data and run cryptographic primitives
Performance & Availability	• **System management:** centralized reissuance of tokens with a long transaction history by the NBK's Node on demand vs distributed reissuance by Nodes of FI/EP • **Payment system:** instant payments vs transaction duration in existing payment systems	**Infrastructure:** • Server-based vs. cloud-based (Kubernetes) • Manual scaling of servers and network vs using Kubernetes automatic scaling	-	• Reissuance of tokens • Throughput measurements on the pilot project load	• Using event streaming of external events to balance the load on API requests to the DLT network • Reissuance of tokens with long transaction history and archiving of old tokens (not in circulation) in the NBK node repository • Selection of technology and consensus mechanism to provide horizontal scaling of nodes • Load and stress testing of the system at the production load level (latency, maximum load)

Principle	Strategic forks	Technological solutions	PoC design	MVP and R&D Design	Potential vision
Stability & Observability	**System management:** the NBK is ready and able to guarantee the level of stability of the platform, legally and financially (quick-and-dirty vs thoughtful and thoroughly tested solution	**Infrastructure:** the ability to create geographically distributed data centers	Limited logging functionality	Using specialized solutions for logging and monitoring	• Creating high availability clusters (geographically distributed data centers) • Availability of SLA testing for the production phase • Testing of the data recovery plan, backup, and migration procedures • 24x7 incident support and management (based on alerting, monitoring, and logging tools)

Appendix 2

Choosing a survey method (Web Survey)

To build a micromodel for assessing the elasticity of substitution of the digital tenge and determining the potential demand for the national digital currency being developed, NAC Analytica conducted a web survey of Kazakhstanis on a given topic (with quotas by region).

The survey method was not chosen by chance but based on world practice in this area. In almost all studies on payment instruments and digital currency, the dominant survey method was a quantitative online/web survey. For example, population surveys in Canada (Carlos Arango & Angelika Welte, 2012), (Christopher S. Henry and Kim P. Huynh and Angelika Welte, 2018), (Marie-Hélène Felt & David Laferrière, 2020), the UK (Natalie Ceeney, 2018), the Netherlands (Bijlsma et al., 2021), Russia (Centre for Research in Financial Technologies and Digital Economy SKOLKOVO-NES 2019) were conducted in the online/web survey mode using quotas. In addition, international comparative studies in developed and developing countries (OMFIF 2020), (and OMFIF 2021) were also carried out using this method.

The research question's specifics determined the choice of the survey method by these countries and organizations. The results of numerous representative studies in different countries demonstrated that the most active users of banking services are people under the age of 45 who live in urban areas and have higher education. Thus, the parameters of the target audience of potential digital currency users are the same as those of active users of the Internet space, in connection with which the online data collection method was chosen.

The experience of other countries has shown that the survey mode in this area does not significantly affect the results. For example, Canadian researchers conducted surveys online and through a representative telephone survey. The results showed the objectivity and reliability of the data obtained in these two modes (when comparing surveys with each other).

As for Kazakhstan, this method is also applicable in our country since official data states that the share of Internet users already exceeds 90%.

In general, it should be noted that the web survey mode has several advantages, such as the speed of data collection, lower cost compared to other methods, the lack of influence of the interviewer on the results of the survey, as well as ensuring maximum anonymity of respondents.

Microeconometric analysis based on Li's (2021) structural demand model made it possible to assess the potential demand for the DT in Kazakhstan compared to its close alternatives. The DT, cash, and deposits are considered to be a group of products with different attributes/characteristics. Household gains from owning each product depend on product characteristics such as convenience, cost of use, security, level of ubiquitous adoption, anonymity, budgeting, household characteristics, and unobservable individual household preferences. The household preferences for each product were assessed based on survey data. The responses contain information about the shares of cash and deposits in liquid assets. Also, respondents stated their ratings on the characteristics of products. Further, assuming that people's preferences remain unchanged after the DT release, the demand for the DT was predicted based on its design characteristics and households' ratings of each attribute.

The same model estimated the constant elasticity of substitution between the DT and cash. The methodology for estimating the elasticity of substitution is based on the fact that households derive utility from holding cash, deposits, and the DT. Assuming that cash and the DT are close substitutes, a utility function with constant household elasticity of substitution consists of holding cash, deposits, and the DT.

Assuming a budget constraint on household liquid assets consisting of the sum of all cash, deposits, and the DT, the elasticity of the substitution equation between cash and the DT was derived by solving the first-order conditions of the Lagrange equation, according to Li (2021). Since the CBDC has been a new concept for the world in the last few years, economic research on this topic is limited. An international literature review has shown that an empirical assessment of the elasticity of substitution between CBDC and cash has not yet been carried out. However, theoretical studies within DSGE models do exist.

The probability of accepting the DT was predicted using logistic regression. The success of the DT implementation depends on understanding what qualities of payment instruments are most important from the point of view of consumers, as well as factors that increase the likelihood of using the DT.

The logistic regression model was constructed to study consumer attitudes toward implementing DT. It assessed the impact of various socio-demographic factors, knowledge of the DT, awareness of cryptocurrencies, the importance of various characteristics of the DT, ease of use of cash and anonymity, and trust in one's bank and the NBK. It also analyzes consumers who frequently use cash and mobile apps to make payments. The dependent variable is the respondent's willingness to use the DT. The variable is built based on the survey question: "If tomorrow a digital tenge is introduced in Kazakhstan, with what probability would you use it?". This is a binary variable that takes the values 1 for respondents' answers "Definitely yes" or "Most likely yes," and 0 for answer options "Not sure," "Most likely not," or "Definitely not."

	Convenience	Price	Security	Anonymity	Acceptance	Budgeting	Bank Configurations	Deposit Interest
Basic design	Cash	Cash	Cash	0,7	1	0,7	0	0
Design similar to cash	Cash	Cash	Cash	1	1	1	0	0
Design similar to a card	Bank Card	Bank Card	Bank Card	0	Bank Card	0	1	Deposit Rate

DSGE models for assessing the impact on macroeconomics, financial stability

Using an estimate of constant elasticity of substitution, the DT is embedded in a medium-scale dynamic stochastic general equilibrium (DSGE) model for Kazakhstan to analyze shock transmission mechanisms and the effects of DT on macroeconomic stability and household welfare as measured by a loss function.

A DSGE model was built with the banking sector to analyze the transmission mechanisms of financial shocks in the presence of the DT and the impact of the DT implementation on financial stability.

It is necessary to build a theoretical model of the Kazakhstan economy to analyze the impact of potential the DT introduction on macroeconomic and financial variables. Empirical models require observations on the DT economy over a relatively long period. Due to the novelty of the DT in the economy and the lack of observations on the digital currency economy, we are building DSGE models for Kazakhstan, in which households use the DT as a means of payment and cash and non-cash funds. These models allow us to experiment with alternative the DT implementations within the models and measure their impact on macroeconomic and financial variables in equilibrium. Microeconometrically, the models, in turn, allows us to estimate the constant elasticity of substitution between the DT and cash in Kazakhstan and use this parameter within DSGE models.

The novelty of this study is that the models take into account not only the unique structure of the economy of Kazakhstan through equations but also the specific perception of households of the DT and cash in Kazakhstan. Compared to other studies on CVD in DSGE models, we estimate the constant elasticity of substitution through a micro-econometric model and use it in the DSGE model. In contrast, other studies fix the coefficient of elasticity of substitution at values not supported by empirical estimates.

In general, there are only a limited number of studies analyzing the presence of CBDC in the DSGE model. Barrdear and Kumhof (2021) analyze the macroeconomic and welfare impacts of CBDC implementation using a DSGE closed economy model calibrated for the US economy. They conclude that GDP grows by 3% steadily with the introduction of the CBDC. However, the closed economy model is less relevant for Kazakhstan since our economy is more susceptible to external shocks, making it relevant to consider the features of an open economy in the model. George et al. (2018) and Minesso et al. (2022) build DSGE open economy models with the DT to analyze shock transmission mechanisms depending on the characteristics of the CBDC. Minesso et al. (2022) conclude that implementing the CBDC in the Eurozone will lead to a more volatile euro exchange rate against other currencies. Burlon et al. (2022) build a DSGE model with the financial sector and CBDC. They conclude that GDP falls in real terms at a steady state for the Eurozone with the introduction of the CBDC but also observe a flattening of the response of lending and GDP to shocks in the economy. Gross and Schiller (2021) also examine the impact of the CBDC on the banking sector in the economy. They conclude that the CBDC can crowd out bank deposits, but the central bank can control this outflow of funds from CBDC deposits by changing the interest rate on the CBDC. In this report, we build on existing DSGE models - Abilov and Rahardja (2022) and Gerali et al. (2010) and modify them to include the CBDC in the model. This report uses these models to analyze the economic impact of introducing DT in Kazakhstan.

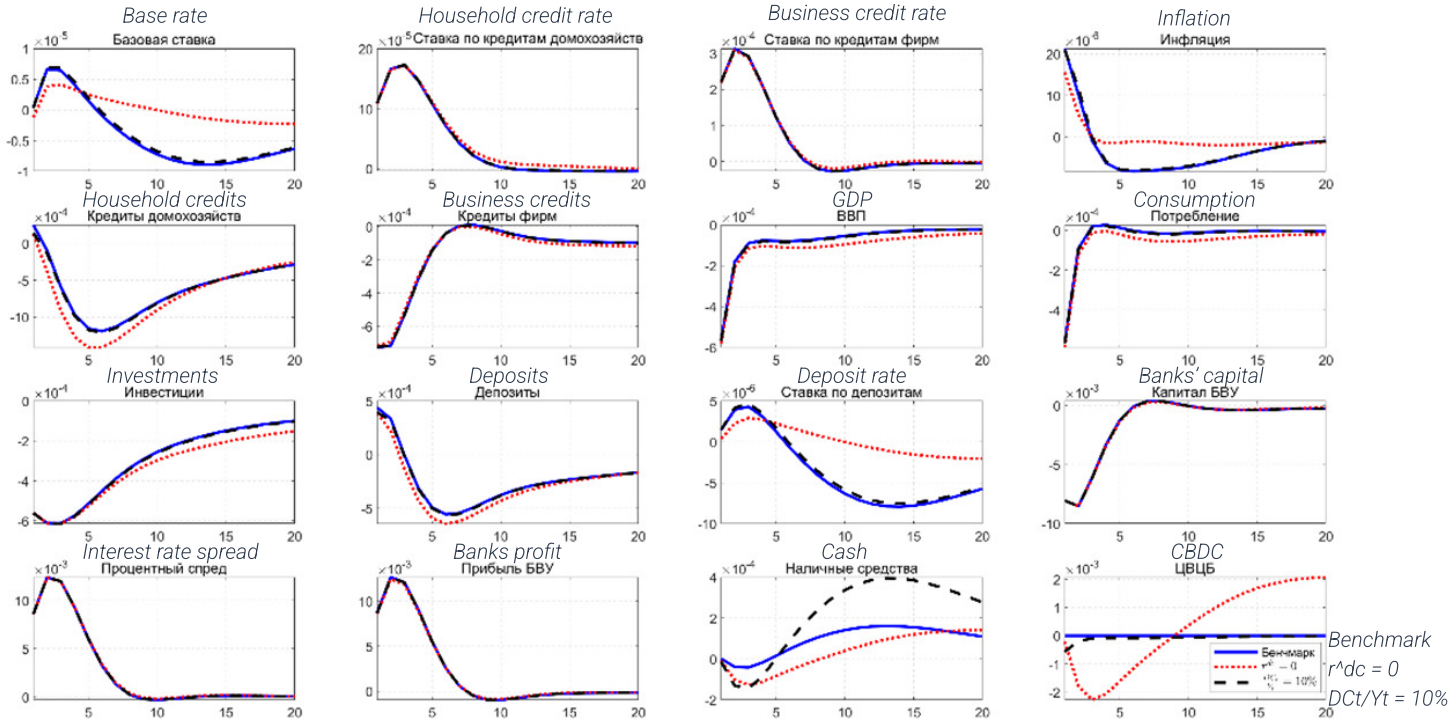
The transmission mechanisms for financial shocks are virtually unchanged due to the close fungibility of cash and the DT. The impulse responses of key macroeconomic variables in the baseline scenario without DT and those with the DT differ only in magnitude but not in the direction of impulse responses. From the point of view of financial stability, the optimal amount of DT is 10% of the annual GDP. On the other hand, the zero interest rate on the DT rule improves the macroeconomic environment compared to other DT rules because the economy is more stable, and the welfare of households changes insignificantly.

The model's impulse response functions show that a one percentage point increase in the DT to GDP ratio increases the annual inflation rate by 0.2 percentage points in the same quarter, with the effect gradually fading in subsequent quarters.

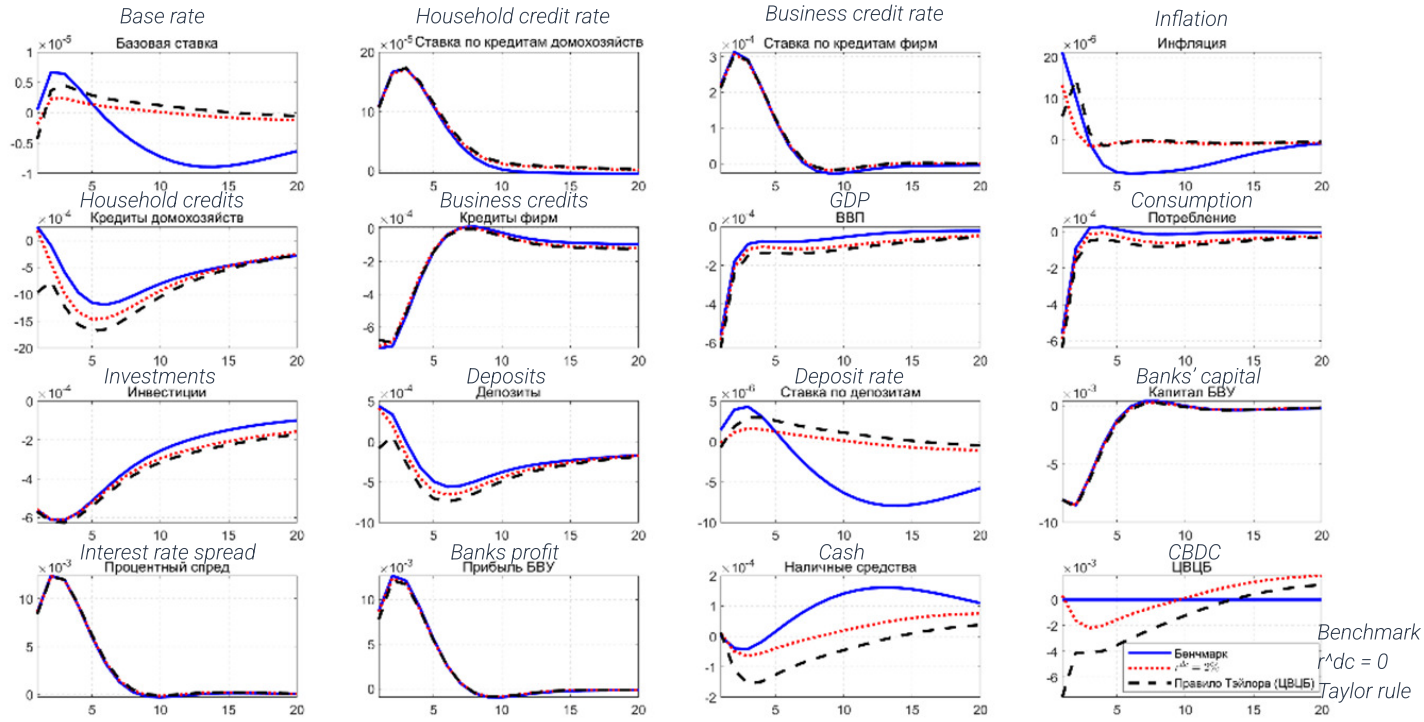
Figure below shows that the DT implementation allows the CB to influence the economy by issuing and withdrawing the DT from the economy. In this case, due to imperfect complementarity (constant elasticity less than 1 and equal to 0.735), cash and the DT move synchronously, and therefore liquidity in the economy reacts more strongly. When the base rate changes, the costs of holding assets in cash and the DT also change. Therefore, a change in the base rate leads to a change in the amount of cash and the DT required by households. However, since they are complementary kinds of instruments, a change in 1 spurs a change in the other instrument in the same direction, i.e., a feedback effect is created. In other words, when the central bank changes the base rate, the amount of liquidity changes more because of the complementarity of cash and the DT. As a result, banks are responding by changing lending rates to a greater extent, resulting in more pronounced changes in consumption and investment. This leads to a more pronounced reaction of GDP and inflation in the economy. The increased responsiveness of macroeconomic variables to the base rate means that the CB can have a more significant economic impact when the DT is implemented.

Figures show the impulse responses of the selected variables to a negative bank capital shock under the baseline scenario and four alternative CBDC scenarios. The responses under the zero interest rate CBDC and the fixed CBDC to GDP ratio are almost identical to the impulse responses under the base case. The difference arises in the responses of cash and CBDC. On the other hand, scenarios with a fixed interest rate on the CBDC and the Taylor rule for the interest rate on the CBDC show little difference in the magnitudes of the impulse responses of the endogenous variables. However, the directions of the impulse responses are similar to the base scenario. A negative shock to bank capital worsens the capital-to-assets ratio of banks.

Consequently, they respond by raising deposit and lending rates. Higher interest rates on deposits attract depositors' savings and compensate banks for their loss of equity. Higher interest rates on loans widen the spread and result in higher profits for banks, which can be used to build bank capital. On the other hand, higher interest rates reduce the demand for loans from borrowers and entrepreneurs. As a result, we are seeing a decline in private investment and consumption. However, the negative impact on consumption quickly disappears within 3 quarters due to low hardness. However, output and investment remain below their sustainable levels for extended periods. Investment returns to a steady state only after 20 quarters. Inflation rises in response to an increase in firms' marginal cost due to lower capital accumulation and higher demand for labor services. The CB reacts by raising the base rate to counter the effect of rising inflation. In all CBDC scenarios, except for the fixed CBDC/GDP scenario, cash and CBDC are subject to adjustment after the shock effect disappears. At the same time, with the CBDC at 10% of GDP, these liquid assets adjust much faster over 5 quarters.



Impulse responses when the base rate increases



Impulse responses to the negative shock of STB capital

Note:

1. Weight means the weight of the variables in the overall loss function
2. The values in the table are distributed from 1 to 4, where "1" is the most stable scenario, and "4" is the least stable

Production volume and inflation rate											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	1	1	1	1	1	1	1	1	1	1	1
Issuing the DT as 10% of GDP	2	2	2	3	4	4	4	4	4	4	4
The DT with a fixed rate of 2%	3	3	3	2	2	2	2	2	2	2	2
The DT with variable rates, where the interest rate is determined through Taylor's rule	4	4	4	4	3	3	3	3	3	3	3

Output and the real exchange rate											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	1	1	1	1	1	1	1	1	1	1	1
Issuing the DT as 10% of GDP	4	4	4	4	4	4	4	4	4	4	4
The DT with a fixed rate of 2%	2	2	2	2	2	2	2	2	2	2	2
The DT with variable rates, where the interest rate is determined through Taylor's rule	3	3	3	3	3	3	3	3	3	3	3

Output and the budget deficit											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	1	1	1	1	1	1	1	1	1	1	1
Issuing the DT as 10% of GDP	2	2	2	2	2	2	2	2	2	2	4
The DT with a fixed rate of 2%	4	4	4	4	4	4	4	4	4	3	2
The DT with variable rates, where the interest rate is determined through Taylor's rule	3	3	3	3	3	3	3	3	3	4	3

Note:

1. Weight means the weight of the variables in the overall loss function
2. The values in the table are distributed from 1 to 4, where "1" indicates the most stable scenario and "4" means the least stable

Capital adequacy											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	2	2	2	2	2	2	2	2	2	2	2
Issuing the DT as 10% of GDP	1	1	1	1	1	1	1	1	1	1	1
The DT with a fixed rate of 2%	3	3	3	3	3	3	3	3	3	3	3
The DT with variable rates, where the interest rate is determined through Taylor's rule	4	4	4	4	4	4	4	4	4	4	4

Return on assets											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	2	2	2	2	2	2	2	2	2	2	2
Issuing the DT as 10% of GDP	1	1	1	1	1	1	1	1	1	1	1
The DT with a fixed rate of 2%	3	3	3	3	3	3	3	3	3	3	3
The DT with variable rates, where the interest rate is determined through Taylor's rule	4	4	4	4	4	4	4	4	4	4	4

Return on equity											
Scenario/Weight	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
The DT with zero zero interest rate	2	2	2	2	2	2	2	2	2	2	2
Issuing the DT as 10% of GDP	1	1	1	1	1	1	1	1	1	1	1
The DT with a fixed rate of 2%	3	3	3	3	3	3	3	3	3	3	3
The DT with variable rates, where the interest rate is determined through Taylor's rule	4	4	4	4	4	4	4	4	4	4	4

Note:

1. The values in the table are distributed from 1 to 2, where "1" means that the responses of important macroeconomic and financial variables are less expressed from the baseline scenario without DT.
2. A value of "2" means that the responses are more expressed from the baseline scenario. Similarly, the value "2" is given to several scenarios at once, as the answers in these scenarios are comparable.

	Macroeconomic stability		*Financial stability*	
Scenario/Shock	***Monetary policy***	***Oil price***	***Monetary policy***	***Bank capital***
The DT with zero interest rate	*1*	*1*	*2*	*2*
Issuing the DT as 10% of GDP	*2*	*2*	*1*	*1*
The DT with a fixed rate of 2%	*2*	*2*	*2*	*2*
The DT with variable rates, where the interest rate is determined through Taylor's rule	*2*	*2*	*2*	*2*

Approaches to risk elimination

According to the latest BIS research, the proposed measures to address the risks of a flow of funds to the CBDC fall into quantitative and price measures.

CBDC design options to moderate take-up

Quantity measures/ limits	Max. holding limit	Differentiated limits	Transaction limits
Price measures/ remuneration	Unremunerated / Negative remuneration	Tiered remuneration	
In-crisis measures	Gates/switching limits	Banking support	

Quantitative measures will limit the use of CBDC by imposing restrictions on the transfer and storage of CBDC. Quantitative limits can be either on a volume basis (central banks limit the number of CBDCs held by individuals/individual account holders) or on a flow basis (limits on the number of CBDCs that can be transferred in a given period, e.g., per day, account holder). Levels of quantitative limits can be set, taking into account the volume of cash circulation and payments in households.

Price measures can be used to reduce the holding capacity of the CBDC or large payments in the CBDC (without limiting them). The reward system can be either single-tier or multi-tier. In a single-tier system, CBDC holders would be rewarded at the rate regardless of the amount held. In a two-tier system, up to a predetermined threshold amount (q1), CBDC owners will pay a sure profit (r.); the amount held more than q1 will be rewarded with a lower yield (r2<r1). Central banks will need to decide how to apply interest rates (for example, on a spot basis or an average over a period), considering technical possibilities. In addition, central banks could consider charging a fee (fixed or progressive) for CBDC transfers above a certain amount.

Combinations of measures are also considered. For example, a central bank might consider a two-tier remuneration system with restrictions on the amount of CBDC that can be transferred on a certain day.

Whether implemented in parallel or not, the presence of the above design features will reduce the attractiveness of the CBDC as a savings instrument and thus reduce the degree of disintermediation and possible subsequent risks to financial stability.

Restrictions may also apply differently for different CBDC account holders, entrepreneurs, and households. For example, tighter business restrictions could reduce the overall use of the CBDC while maintaining access to financial services for ordinary citizens.

Such restrictions may be imposed permanently or temporarily. Some central banks may consider structurally limiting the use of CBDC and the risks associated with substitution with private money. Others may use transition measures only to slow initial uptake and give the financial system time to adjust.

Central banks will assess the required volume of the CBDC, taking into account the risks of an overflow of funds from current accounts and deposits to the CBDC. This level may vary depending on the jurisdiction and its financial structure. All restrictions will take into account the fundamental goals of implementing the CBDC, providing the population with access to secure means of payment, expanding coverage and accessibility, or encouraging competition around the CBDC which are the part of its economic benefits.

Source: BIS - Central bank digital currencies: financial stability implications September 2021

The implementation of limits requires access to relevant data (even if automated) and additional processing. In some cases, legal and political issues may need to be considered in connection with the premise of imposing restrictions and/or negative interest rates on household property owned by the public.

Banking risk management measures

Prudential regulation is under constant review as the liquidity of bank deposits and other liabilities changes over time, for example, due to technological innovations. Introducing CBDCs or new forms of private money, such as stablecoins, may affect the hidden risk of systemic launches, and banks may also need to adapt their practices (Juks (2018)). For example, in the current LCR rules, the outflow parameters for deposits provided by retail and small business clients were set based on observed outflow rates during periods of stress, which, by definition, do not take into account the impact on the behavior of depositors under stress in the presence of the CBDC or some new private forms of digital of money. Suppose the CBDC implementation increases the risk of an outflow for such deposits. In that case, the applicable outflow rates may need to be revised to ensure sufficient liquidity to cover potential outflows during times of stress.

The authorities may also need more rapid crisis management tools and a review of anti-crisis measures, such as restrictions or controls on the outflow of funds from bank deposits. The framework for providing liquidity by central banks may also be revised, for example, to increase provision or access.

Other measures

To the extent that the introduction of the CBDC or new private forms of digital money introduces new trends, strategies, regulations, rules, or competitive advantages in the provision of services by various players, new concentrations of service provision may arise. Central banks must be confident that the legal framework and oversight mechanisms will support effective monitoring and regulation as the system evolves.