



NATIONAL BANK OF KAZAKHSTAN

DIGITAL TENGE PROJECT



WHITE PAPER ON PROJECT RESULTS
2021

Abbreviations

AML/CFT	Anti-money laundering / Combating the financing of terrorism
API	(Application programming interface) A description of the ways where one computer program can interact with another program
CBDC	Central Bank Digital Currency
DeFi	(Decentralised Finance) is a blockchain-based form of finance that does not rely on central financial intermediaries such as brokerages, exchanges, or banks to offer traditional financial instruments, and instead utilizes smart contracts on blockchains
DLT	(Distributed ledger technology) An approach to the exchange and storage of information on a non-fixed number of communication nodes using predetermined consensus algorithms to synchronize copies of data between participants
DT	The DT
ICS	Interbank clearing system
IoT	(Internet of things) A set of technologies that connect devices into a network and allow them to collect, analyze, process and transmit data to other objects through software, applications, or technological devices, for example, initiate banking transactions
ISMT	The Interbank System of Money Transfer
KYC	(Know your customer или Know Your Client) Customer identification procedure
NBK	National Bank of the Republic of Kazakhstan
P2P	(Peer-to-Peer, Person-to-Person) Network by which computers operated by individuals can share information and resources directly without relying on a dedicated central server
SIP	National Payment System of Instant Payments
STB	Second-tier banks
UTXO	(Unspent transaction output) The output of unspent transactions, i.e. digital currencies that a user receives from each transaction. Used in a blockchain system

Glossary

Report	The DT public discussion report (May 2021)
Interoperability	The ability of a product or system, the interfaces of which are completely open, to interact and function with other products or systems without restrictions on access and implementation
Consensus	A set of certain mathematical rules and functions that govern the operation of the network. Consensus ensures the integrity and security of transactions in a distributed ledger by signing and validating transactions by all participants in those transactions
Light clients	Network participants (nodes) who can act in transactions and sign them fully on their own, while these are participants with limited functionality relative to basic platform clients (in terms of storing a full copy of the registry, validating transactions and the ability to add and launch applications of Corda)
Node	A host – a device connected to other devices as part of a network
Survey	Survey of future potential users of DT and DT platform to determine the properties of the DT. It was carried out during the pilot project to identify the necessary characteristics of the DT and DT tokens in particular
Offline payments	In this document: payments without Internet connection for both parties of the transaction
Pilot platform	A prototype of the DT platform with a limited number of emulated participants, designed to test the main scenarios of the DT life cycle
Pilot project	Project for prototype platform development (pilot platform) to test the viability of the DT concept
Program	Program for the development of the national payment system in the Republic of Kazakhstan until 2025
Distributed ledger	A set of databases with financial transactions and mechanisms for accounting for these transactions based on cryptographic functions
Smart contract	A computer algorithm, a programmed contract, terms of which are written in the program code, and which is automatically executed using blockchain technology
Token	The state of recording in the registry at a certain point in time, the value of the token is inherent in it and is confirmed by cryptographic operations within the distributed ledger
Ecosystem	In this document: A set of processes of interaction with external market participants during the pilot project

Content

Acknowledgement, feedback	5
Executive summary	6
Introduction	7
1. Preconditions and development of CBDC in Kazakhstan	10-23
1.1 Historical preconditions and trends in payment industry	10
1.2 CBDC compared to other forms of money	12
1.3 CBDC advantages and opportunities	14
1.4 The DT: preconditions and approach to introduction	15
2. Pilot project results	25-71
2.1 Review of the DT pilot project	25
2.2 Roles, participants and architecture of the pilot platform	29
2.3 Choice of technological solution (DLT platform)	32
2.4 Pilot project scenarios	33
2.5 Technical aspects for further elaboration	64
2.6 Comparison with CBDC projects in other countries	69
3. Economic and regulatory aspects	73-90
3.1 Economic aspects	73
3.2 Regulatory aspects	83
3.3 Wholesale transactions	89
3.4 Cross-border payments	90
4. Further steps	92-95
An approach to further investigations	92
Expert feedback	96
List of references	98

Acknowledgement

The research work on various aspects of DT implementation is conducted in close cooperation with international organizations and the world's leading experts studying central bank digital currencies.

The National Bank acknowledges the valuable contributions and support of international partners and the expert community in conducting the study:



Expert feedback



"The paper should be a shining beacon and light for other central banks, NGOs, academics, digital currency, cryptocurrency enthusiasts and anyone else that is looking to absorb some fresh and deep perspective on how a CBDC potentially can be implemented by a team like the NBK that is nothing less than genius".

Professor Jamiel Sheikh

Founder The Central Bank Digital Currency Think Tank, professor at Columbia Business School



"I commend the NBK on the delivery of this excellent report. The paper highlights answers on critical questions such as regulatory implications, application of DLT as mitigation for risk of central points of failure and application of programmability".

Willy Lim

Global Advisory Lead – Digital Currencies and Capital Markets, R3

Executive summary

This document presents the results of the first phase of the pilot project on the national digital currency implementation of the Republic of Kazakhstan. The project was launched in 2021 in close cooperation with financial market participants, expert community, and international partners.

The digital tenge will be the third form of the national currency of Kazakhstan along with cash and its cashless form. The digital tenge will become an additional digital payment instrument for business participants guaranteed by the National Bank of the Republic of Kazakhstan.

The key motivation in the digital tenge study is its potential to improve financial inclusion, promote competition and innovation in the payments industry, and increase the competitive advantages of Kazakhstan's financial sector compared to the global market.

The main objectives of the pilot project for 2021 included the test of the feasibility of the DT concept through the experimental confirmation of the technological realization based on distributed ledger technology as well as the definition of the core CBDC model parameters for Kazakhstan together with all stakeholders.

As part of the pilot project, basic DT life cycle scenarios were implemented - from issue and distribution to purchases and transfers using DT. Among the achieved advantages of the implemented technological solutions are the following:

- tokenization of ownership – the DT is stored by the user in the form of tokens in a digital wallet on the mobile device (or another gadget) which enables full control over money
- offline payments – DT users can make purchases when both the customer and the merchant do not have Internet access
- customizable anonymity – transaction details can be hidden from all settlement participants (including at the user's choice) while ensuring a possibility to carry out necessary checks
- special purpose tokens – the programmability of

the DT allows to put restrictions on spending in token structure and simplify tracking of its use on special purposes

- simplicity of integration - DT infrastructure provides an opportunity for easy connection and implementation of their scenarios for traditional (STB) and new (fintech) financial market players.

The study is based upon the global experience of other central banks that have made significant progress in tokenized retail digital currencies. It also leveraged the expertise of the pilot project technology partner, Accenture, which has advanced experience in implementing projects in the field of digital currencies in Sweden, Singapore, Canada, Eurozone, USA, Switzerland, South Africa, and other countries.

As a result of the project, hypotheses about the technological feasibility of the DT concept were confirmed and a list of questions and tasks was identified for further development. In addition, a primary model was developed to evaluate the impact of the DT on the economy, financial stability, and monetary policy as well as possible approaches to regulation.

The decision-making framework for CBDC issuance in Kazakhstan will be determined in July 2022. The priority of NBK in the decision development will be an assessment of benefits for payment services consumers.

The resolution on the need of the DT introduction will be made at the end of 2022 based on results of a comprehensive study of potential benefits and risks, elaboration of technological aspects, the impact on monetary policy and financial stability, as well as the effect for the National Payment System and its participants.

This paper sets out the NBK's study results on the potential implications, benefits, and risks, organizational and technological opportunities of central bank digital currency introduction in Kazakhstan.

The report intends to inform the general public, professional market participants, and the financial community about key results of the pilot project, possible DT functionalities as well as economic aspects of DT implementation.

Key milestones of the pilot project in 2021

- May, the Digital Tenge Public Discussion Report was released
- May - December, special meetings and discussions with market participants, expert community, government agencies as well as international organizations and central banks were held
- June, a pilot project was launched to assess the technical feasibility of DT, during which a prototype platform was implemented and several scenarios were tested involving external participants with the participation of two banks
- September, surveys, and interviews with market participants were conducted to clarify priorities and needs in the development of new payment instruments
- November, preliminary results of the pilot project were presented within the IX Congress of Financiers of Kazakhstan
- December, the current report on the results of the pilot project was prepared.

This report consists of 4 key sections

- the first part outlines the prerequisites for the emergence of CBDC, their features, and advantages, as well as the key characteristics of the DT in the context of the National Payment System of Kazakhstan
- the second part of the paper reveals the main results of the pilot project aimed to assess the technical feasibility of the DT concept, including a description of the chosen approach, implemented scenarios, key architectural solutions, and aspects for further elaboration
- the third part of the report describes the results of the study of the economic and regulatory aspects of the introduction of DT
- the fourth part outlines the approach and further steps to elaborate on the issue of the introduction of DH in Kazakhstan.

2021



MAY

5 May release of the report, invitations for 12 May
12 May discussion with the market
31 May publication and distribution of answers to questions from participants of the discussion

JUNE

15-29 June discussions with other Central Banks, discussions within the CBDC Think Tank, discussions with the IMF

JULY

14 July sending an invitation to a profile meeting through the AFC with a presentation which sets out requirements to joining the pilot
16 July discussion with the Central Bank of Hungary
23 July profile meeting with BWU invitation to the pilot, discussions with WEF

AUGUST

3 August receiving from AFC a list of second-tier banks willing to join the pilot
5-12 August task discussions with STB on participation in the pilot
24 July -12 August calling STBs to clarify the requirements
24 August sending an invitation to STBs to a profile meeting due on 27 August
27 August profile meeting with STBs, distribution of presentation, invitation to interview and next profile meeting on 17 September
3 August discussion of China's CBDC within CBDC Think Tank, discussions with the IMF

SEPTEMBER

2-15 September online survey of STBs
6-14 September interview with STBs
17 September profile meeting with STBs, presentation of answers to questions of STBs consolidated during interviews
9 September Global CBDC Challenge Masterclass Singapore Fintech Festival

OCTOBER

4 October discussion with representatives of the US Diplomatic Mission
4-6 October CBDC academy Lighthouse Communications LLC
6 October BIS Conference FSI-IOSCO
21 October discussion with the Central Bank of Sweden, discussions with BIS, IMF

NOVEMBER

12 November plenary session at the IX Congress of Financiers with participation of representatives of Accenture, R3, IMF, WEF
23 November discussion of the Norwegian CBDC project within CBDC Think Tank, discussion with the IMF

DECEMBER

15 December release of the final report

2022



Preconditions and development of CBDC in Kazakhstan

pages **10-23**

Formation of money function

Money's existence stretches back to the periods, when it appeared in a tangible form, including all kinds of valuable things such as bars and coins made of precious metals or other materials that were practical in use. At this stage, money functioned as a means of exchange and an accounting measure, which made it possible to overcome a problem of 'double coincidence of need' in barter exchange.

Furthermore, the development of banking established the following important function of money - to serve as a store of value. For the convenience of storage and settlements, banks began to issue their currencies, the value of which was usually secured by material assets stored in a bank. Meanwhile, it was impossible to reliably verify the correspondence between the value of the currency and the funds in the bank vault. The use of funds depended on the degree of trust in their issuer: the willingness to accept a particular currency was determined by a person's confidence in a particular bank.

In the second half of the 20th century, the desire to have a universal means of payment independent of the actions of private financial institutions led to the emergence of the modern concept of fiat money issued and guaranteed by the central bank.

Digitalization

Advances in computer technology have contributed to the further development of banking services and have led to the emergence of electronic payments and a cashless form of money.

Cryptocurrency is a digital asset based on distributed ledger technology (DLT) and blockchain. Cryptocurrencies do not have a single issuer: their issuance is decentralized.

A new milestone in the development of financial markets was the advent of cryptocurrencies in the early 21st century. The next generation of technology-enabled the possibility to transfer value electronically without double-spending and financial intermediaries. However, despite the technological advantages of cryptocurrencies, their market capitalization is subject to significant fluctuations, pricing is not transparent enough, and legal status remains uncertain, which limits their use as a means of payment.

Stablecoins, which have artificially fixed exchange rates, have been able to solve some of these problems. However, by their nature, stablecoins remain private, unsecured assets.

Stablecoins – cryptocurrencies value of which is pegged to value of another, more stable asset, usually to an exchange rate of some government currency through liquidity provision or algorithmic means.

The massive rise of the cryptocurrency market prompted the exploration of decentralized finance (DeFi). DeFi is based on blockchain and smart contracts and does not rely on intermediaries and centralized institutions. The benefits often quoted in the context of DeFi include democratization, increased accessibility, flexibility, and complexity of financial transactions. At the same time, DeFi can pose high risks for some groups of people, who are unaware of risks and can lead to the loss of a significant share of savings.

In response to these risks and challenges, central banks around the world have begun to explore the possibility of creating their own digital currencies that will combine the traditional functions of money with the technological demands of today's digital economy in a way that meets the interests and needs of all economic actors.

Thematic quarterly review from the Bank for International Settlements released in April 2021 recorded 65 CBDC research projects around the world, and an update of review in October 2021 already mentions 84 projects. The number of pilot projects during this period increased from 9 to 26 [\[26\]](#).

1.2 CBDC compared to other forms of money

CBDC is a digital payment instrument and is a liability of the central bank. Being a store of value and payment instrument token-based CBDC represents the third form of national currency. It combines several features of cash and non-cash payment instruments and complements them with new functionalities for business participants and government institutions.

1. CBDC and cash

Advantages of cash:

- ✓ they are direct liabilities of the central bank
- ✓ simplicity (when a buyer hands over a banknote to a seller, monetary value is transferred instantly and the transaction is finalized immediately without financial intermediation and subsequent settlements)
- ✓ anonymity (seller and buyer do not need to know any additional information about each other, such as bank account number or cell phone number)
- ✓ payments without an Internet connection.

However, the advantages of cash turn out to be disadvantaged in other situations:

- ✓ inconvenience of using paper bills in settlements (change, when there is no change)
- ✓ inability to make a payment remotely
- ✓ the risks of loss, theft, damage, wear and tear, forgery
- ✓ opportunities for use in illegal activities at the expense of anonymity
- ✓ significant costs related to issuance, circulation, and collection for businesses, commercial banks, and the central bank

The obvious advantages of cash (instant and easy settlements, anonymity, offline capabilities) also apply to CBDC. At the same time, being an electronic form of money, CBDC by default will not have the above-mentioned risks and limitations associated with the material nature of cash.

2. CBDC and cashless payment instruments

In essence, cashless payments represent the exchange of electronic messages: debiting the account of the buyer and their receipt in the seller's account.

Benefits of cashless payments include:

- ✓ ability to make payments without physical contact
- ✓ convenience of storage and access to funds in digital format
- ✓ ease of payment, including the ability to seamlessly integrate payment into the digital user experience on digital platforms and access to payments and transfers through banks' mobile apps

1.2 CBDC compared to other forms of money

✓ services linked to payments (access to invoices, auto payments, loyalty programs, and bonus programs, analytics, and financial management).

However, cashless payments have their limitations:

- ✓ requirements for customer identification and impossibility to make anonymous transactions
- ✓ impossibility to make payments in the absence of Internet connection (including, for example, in the case of interruptions in network connection, power supply, etc.)
- ✓ risks of financial intermediaries which ensure payments and storage of customer funds in the account (as obligations of a commercial organization)
- ✓ deferred finalization of settlements, e.g., for payments through the interbank infrastructure of retail net settlement
- ✓ the costs of commissions of financial intermediaries, for example in acquiring payments through the card infrastructure.





CBDC retains several advantages of cashless payments: payments without physical contact, ability to conduct transactions using a mobile phone, ease of storage and access to digital funds, ability to seamlessly embed payment into the user experience (for a description of the properties of CBDC and DT, please see sections 1.3 and 2 below.).

In addition to the advantages of cashless payments, CBDCs provide a higher level of anonymity (for more detail about anonymity please see 2.4.2.6), support the ability to make offline payments, transfer between wallets instantly, and can be stored directly on users' gadgets (which ensures full control over funds and their safety).

1.3 CBDC advantages and opportunities

The implementation of CBDC will potentially bring a whole new set of digital opportunities and advantages that will benefit all key stakeholder groups: consumers, financial and government institutions.

CBDC advantages and opportunities

 <h3>CITIZENS</h3> <ul style="list-style-type: none">Convenience and ease of the 'digital cash' guaranteed by the central bankExpanding the availability of payments (for ex. in remote regions or during the temporary unavailability of the Internet)Lower fees for payments and remittancesImproved security and reliability of payments	 <h3>BUSINESS</h3> <ul style="list-style-type: none">Lower cash handling costs and transaction feesOptimization of a billing cycle, increased speed and efficiencyRisks mitigationNew services and new possibilities for settlements due to programmability and offline payments
 <h3>FINANCIAL ORGANIZATIONS</h3> <ul style="list-style-type: none">New sources of income, new services and facilitiesLower cost of cash collectionMitigation of settlement and counter party risksOptimization of a settlement cycleLower costs of cross-border payments	 <h3>STATE</h3> <ul style="list-style-type: none">Improved efficiency of social and government paymentsTransparency and traceability of government paymentsDevelopment of competitionImprovement of financial inclusionDevelopment of innovativeness of the financial sector

EXAMPLES OF POTENTIAL CBDC APPLICATION



Intended use

Special purpose tokens 'matking' of tokens which allows to control the purpose of payments and track usage



Payments involving the state

Reducing the risks of errors, abuse, fraud, the ability to control the intended use, as well as making quick changes to the parameters of social assistance



IoT and M2M payments

CBDC will be a convenient tool for the implementation of direct (without intermediaries) payments between devices IoT objects due to their autonomy and programmability



Pay as you go (pay-per-use, pay-as-you-go)

Through the use of smart contracts, CBDC will provide the ability to pay for the exact, actually consumed amount of products, resources, services, provide the necessary flexibility, savings and control over spending of funds



Micropayments and write-offs on an ongoing basis

The payment properties of CBDC allow implementing incremental payments in pay-as-you-go models with infinitesimal increments, reducing the associated time costs



Supply chain payments

Programmability and traceability of CBDC allows for automatic (including special conditions) and transparent settlements for participants in the supply chain, reducing risks and costs, increasing the level of confidence of participants in the chain

1. Preconditions for the introduction of digital currency in Kazakhstan

The prerequisites for launching the DT project were presented [in the Report](#) for public discussion:

- ✓ **Financial Inclusion.** The need to increase financial inclusion and accessibility of modern digital payments for the category of citizens and businesses with limited access to modern payment services.

In 2021, the share of non-cash payments in the retail turnover of Kazakhstan reached 77% [36]. However, due to the uneven geographical concentration of financial and payment services, a significant part of the population of Kazakhstan, especially in rural and remote areas, still has limited access to financial services and the banking system.

- ✓ **Efficiency of the payment infrastructure.** The potential to improve the existing payment infrastructure. Technological innovations contribute to increasing opportunities for non-cash payments in offline mode; increasing anonymity and privacy in non-cash payments; enabling the general public to hold electronic assets, which are a direct obligation of the state; further increasing the sustainability of the national payment system, since a decentralized infrastructure (based on distributed registry technologies) due to the absence of a central link as a single point of failure is potentially more resilient.
- ✓ **Improvement of payments involving the state.** The task of increasing the efficiency of payment scenarios with state participation is attributed to the active role of the state in national economic development and significant social obligations of the state.
- ✓ **Digitalization of payment infrastructure.** The need to improve the technological adaptability of the payment infrastructure due to the increasing presence of private cryptocurrencies and stablecoins in the financial sector, increased international competition in the development of public digital currencies, the growing role of international technology companies in the financial sector, and digital payments.

Based on these prerequisites and issues, the NBK has identified the main objectives for the development of its digital currency:

- further development of the national financial and payment system
- increasing financial inclusion and accessibility of financial services
- promoting competition in the financial sector and its competitiveness
- creating a technological platform for further digitalization
- ensuring the sustainability of the national payment system
- increasing the efficiency of payments involving the state.

2. DT definition

The digital tenge is a liability of the NBK, issued in electronic form and distributed jointly with market participants within the framework of two-tier financial architecture. It is technologically possible to represent DT in the form of an account or token. DT can be used for retail and wholesale settlements. In a pilot project of 2021, a tokenized form of DT was tested for use in retail settlements. The main motivations behind this approach are described in the May [Report](#) for public discussion.

Key characteristics of the DT

COMBINATION OF MONEY PROPERTIES FOR NEW OPPORTUNITIES



REQUIREMENTS TO PAYMENT SYSTEM

- ✓ 24/7 availability
- ✓ Flexibility
- ✓ Interoperability
- ✓ Reliability
- ✓ Instancy
- ✓ Scalability
- ✓ Safety
- ✓ Confidentiality

3. New possibilities of DT for the National Payment System of Kazakhstan

The DT can become an additional means of payment of the Republic of Kazakhstan. At the same time, the DT platform will provide the infrastructure for payments and transfers in DT along with the existing payment systems of Kazakhstan for non-cash payments. Throughout the development of an approach to DT implementation, it is important to take into account the characteristics and specifics of the existing retail and interbank payment systems and differences from the intended properties and characteristics of the DT platform.

The Interbank System of Money Transfer (ISMT) and the Interbank Clearing System (ICS) are interbank payment systems that provide basic infrastructure for all cashless payments in Kazakhstan. According to the statistics of 2020:

- ISMT covers 90% of B2B payments of banks and non-bank financial institutions, participants in the foreign exchange market, and the securities market.
- ICS covers 63% of the volume of cashless B2B payments of commercial banks and non-bank financial institutions [\[32\]](#).

Final settlements for retail transactions are also carried out through these infrastructure payment systems.

In the sphere of retail payments, it is necessary to highlight the following important payment systems used by the population and businesses in Kazakhstan:

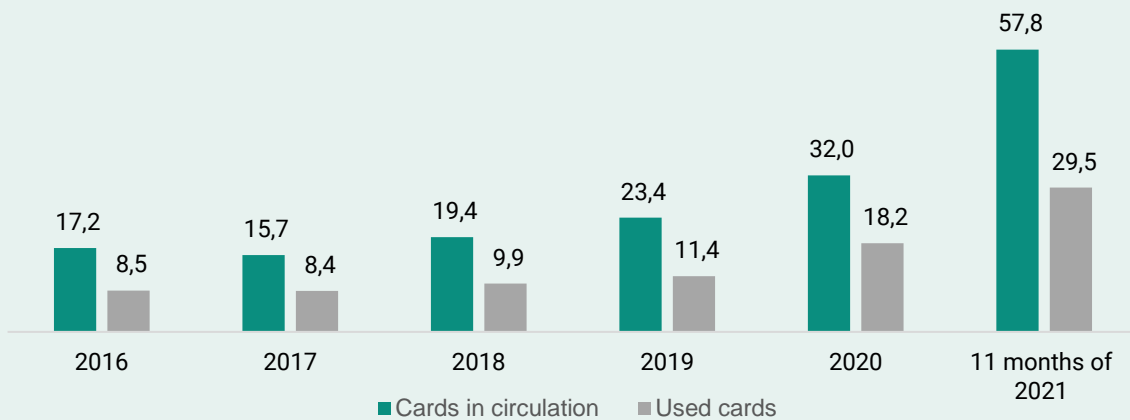
- card payments via international payment systems
- private local payment systems of individual banks
- SMP is a national payment system that provides infrastructure for retail payments and transfers with instant crediting of money to the recipient.

The DT can complement the existing retail payment infrastructure by facilitating the development of new payment services by market participants and the possibility of cashless offline payments. At the same time, the target DT platform will ensure interoperability with the existing payment infrastructure.

Card payments in Kazakhstan

Card payment systems in Kazakhstan mainly include cards issued and accepted for payment by commercial banks in cooperation with two key international card schemes - Visa and Mastercard (other international card systems are also registered and operate, such as American Express, Diners Club, UnionPay, Mir) [\[32\]](#). Card payments and transfers are a convenient tool for cashless payments and cover a full range of needs of citizens and businesses.

Dynamics of issuance and use of payment cards in Kazakhstan (million pieces)



(according to data of the NBK 10.12.2021 [\[32\]](#))

The number of card transactions (which include both transactions with cards of international card schemes and within local banking systems) skyrocketed from 232 million in 2017 to 2.88 billion in 2020. The cash volume of these transactions soared from 3 trillion tenge to 35.3 trillion tenge over the same period [\[33\]](#).

The average amount of transactions slightly decreased from 13.1 thousand tenge in 2017 to 12.3 thousand tenge in 2020. This indicates further development of card payments, despite inflation [\[33\]](#).

Local bank payment systems

Local banking payment systems in Kazakhstan include banking systems that provide payment or transfer within an ecosystem of banks. Such payment systems are closed because they use some variant of on-us transactions when both initiating and receiving parties are clients of the same bank.

The number and volume of cashless transactions within local systems have soared in recent years from 27 billion tenge and 30 thousand transactions in 2017 to 25.6 trillion tenge and 1.98 billion transactions in 2020 [\[33\]](#).

It is important to indicate that transactions within local systems are more than twice as large as transactions with cards of international card schemes, both in terms of quantity and volume. Thus, in 2020, as compared to the aforementioned 1.98 billion transactions for 25.6 trillion tenge, committed within local banking systems, 899 million transactions for 9.7 trillion tenge were carried out through international card systems [\[33\]](#).

Comparison of volumes of transactions via international and local payment

		2016	2017	2018	2019	2020	10 months of 2021
Number of transactions, billion transactions	through international payment systems	0,12	0,23	0,52	0,85	0,90	0,94
	through local payment systems	0,00	0,00	0,00	0,35	1,98	4,1
Transaction volume, trillion tenge	through international payment systems	1,6	3,0	6,3	9,1	9,7	11,9
	through local payment systems	0,1	0,0	0,0	4,9	25,6	45,8

according to data of the NBK as of 10.12.2021 [\[34, 35\]](#)

SIP

The System of Instant Payments provides infrastructure for retail instant payments and transfers [\[34\]](#). The advantages of the system are the availability and speed of transactions for end-users, the limitation lies in the dependence on the participation of banks.

The diversified landscape of the payment infrastructure in the Kazakhstan market and the dynamic growth of non-cash transactions demonstrate opportunities for the development of new payment instruments and further digitalization of payments. The DT can successfully complement the existing payment systems of Kazakhstan by providing users with additional functionality and payment instruments and creating conditions for the competitive development of the financial market.

4. Key principles of introduction

Underlying properties of the DT formulated by NBK are consistent with the basic CBDC principles developed by BIS [\[27\]](#):

Principle 1: Not harm monetary and financial stability

The interests of all participants in Kazakhstan's monetary system will be considered throughout the DT introduction process. The new form of money will contribute to the goals of improving the financial infrastructure without harming the financial stability of the country.

Possible risks to monetary policy and financial stability and technological failures will be analyzed and taken into account in the further development of DT.

Principle 2: Complement existing forms of money

The DT will not compete but will complement the existing forms of money. None of the existing forms of money will be deliberately restricted in circulation. The NBK will continue to supply cash in line with aggregate demand.

Principle 3: Improve payment efficiency and facilitate innovations

Implementation of technological advances is one of the key factors in CBDC implementation. The NBK and all participants in the financial system will prioritize continuous innovation that enhances the efficiency of the payment system.

Also, the design of the DT complies with international principles developed by the G7 (G7 Summit) [\[28\]](#). These public policy guidelines for retail CBDC are an extension of the core principles set by BIS. The G7 principles are divided into two categories:

1) fundamental principles for implementing CBDC:

- availability of legal and regulatory framework
- data protection
- coexistence with existing payment systems
- operational resilience and cybersecurity
- obstacle to illegal financial activities
- stability of the international monetary and financial system
- environmentally friendly use.

2) additional features of CBDC:

- support for innovation in the digital economy
- improvement of financial inclusion
- payments in the public sector
- cross-border payments
- support for international development.

5. Questions for practical research

A well-balanced decision on implementation of the DT requires the assessment of the practical feasibility of a solution that meets the goals and objectives of the introduction of the DT and at the same time does not contradict the key principles (see above).

In 2021 the NBK initiated the development of the DT pilot project where the hypotheses formulated based on previous research were tested.

Interaction between existing challenges and hypotheses

Preconditions and range of problems

▲ Large share of cash in retail payments	▲ Uneven geographic distribution of financial services	▲ Insufficient efficiency of the payment infrastructure, deficit of intersystem interaction
▲ Unfilled demand of the population for reasonable and fast retail payments	▲ Significant costs of the population and business in conduct of cashless payments	▲ Need to improve engineering friendliness of the payment infrastructure

Tasks to develop the National payment system

▲ Efficiency of interbank settlements	▲ Service needs of digital payments	▲ Reduction of aggregate costs of participants
▲ Lower use of cash due to new technologies	▲ Widespread adoption of retail payments	▲ Conditions for competition on the financial market

Objectives of the DT development

▲ Ensure competition on the financial market inside the country	▲ Ensure competitive advantages of the Kazakhstan's financial market	▲ Growing penetration of cashless payments
▲ Operational continuity of the National payment system	▲ Efficiency of state payments	

Confirmed hypotheses

- ✓ Lower costs of money creation
- ✓ User friendly access
- ✓ User friendly ansactions
- ✓ Safe transactions
- ✓ Lower costs of circulation
- ✓ Social payments
- ✓ Programmability
- ✓ Offline transactions
- ✓ Analytics

List of hypotheses to be tested within the pilot project

Hypothesis	Description
Easy access	Mechanism to gain access to the DT system in terms of convenience and security, is not inferior to the existing mechanism of access to the payment infrastructure
Convenient transactions	Mechanisms of payment for DT and transfer of DT, in terms of friendly use and speed of settlements, are not inferior to the existing mechanisms – cash and cashless. And as a maximum – they are more effective in comparison with them.
Safe transactions	Mechanisms of payment for DT and transfer of DT in terms of confidentiality, information security and AML requirements are at least as good as the existing mechanisms – cash and cashless. And as a maximum – they are more effective in comparison with them.
Lower costs of creation	Lower costs in terms of time and costs, compared to the mechanism of cash issuance
Lower costs of circulation	Lower transaction costs associated with systematic accounting of funds at all levels – from the NBK level to digital wallets of individuals and merchants
Social payments	Mechanism to provide the population with social aid in terms of speed, convenience, and traceability of a special purpose spending, at least, is not inferior to the existing mechanism. And as a maximum – they are more effective in comparison with it.
Programmability	The programmable nature of CBDC enables scenarios previously unavailable for cash and cashless payments, including offline transactions, purchases with restrictions (spending on special purposes programmed into the DT's token structure), and other scenarios (external participants) using smart contracts
Offline	Implementation of the possibility of making payments during Internet outages or in regions with insufficient Internet penetration
Analytics	Ability to obtain extended data on transactions in the DT for analysis and simulation of macroeconomic indicators



Pilot project results

pages **25-71**

2.1 Review of the DT pilot project

The DT public discussion report [\[31\]](#) describes the choice of the DT design parameters for the pilot project, where key parameters are:

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	<p>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:</p> <ul style="list-style-type: none">▪ NBK ensures the connection of infrastructure participants (STBs, public authorities, etc.) to the platform▪ STBs ensure the connection of individuals and legal entities through an opening of digital wallets on the DT platform provided by NBK▪ No double-spending, that is, it is impossible to use the same DT in different operations guaranteed by NBK
Token based model	With a token-based model, the use of funds depends on the ability of the payee to verify the validity of the payment object based on the payment network
Two-tier architecture	<p>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.</p> <p>Intermediaries (commercial banks, fintech organizations) interact with end-users: opening and servicing customer wallets, providing retail payments, KYC</p>

The development of a prototype with the specified characteristics enables answering the questions concerning the feasibility of assumptions about the use of distributed ledger technology for CBDC:

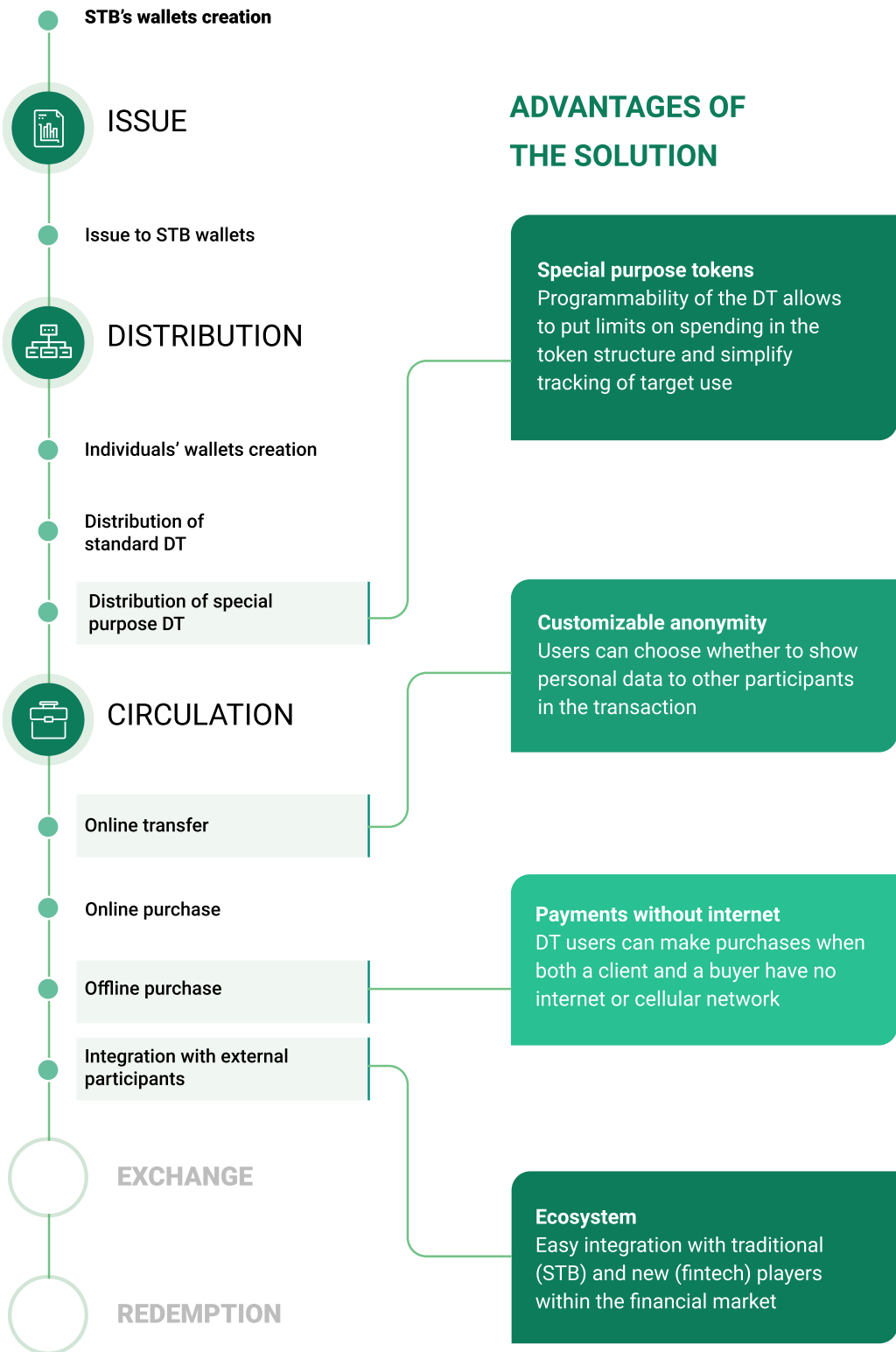
- ✓ Traceability of transactions by participants: transaction participants can verify the validity of the received tokens based on the token's transaction history. Thus, guarantees of verifiability and traceability of the origin of tokens are ensured, which helps to comply with AML/CFT requirements [\[6\]](#)

2.1 Review of the DT pilot project

- ✓ Improvement of transaction reliability: in financial systems which are not based on distributed ledgers, data can be stored centrally, and, despite the possibility of replication and data backup, there is a single point of failure – the infrastructure of a particular bank. In the case of distributed ledgers, each transaction participant retains a copy of the transaction as well as the history of all transactions in the transferred DT token itself. Such decentralized storage reduces the risk of data loss or counterfeiting. However, privacy can be compromised when the transactions information is widely shared by the network. [\[7\]](#)
- ✓ Programmability capacities: distributed ledger architecture enables the creation of smart contracts that can increase the speed of transactions by automating some payments and transfers [\[6,7\]](#). The possibilities of programmability and their use in the pilot project are described in section 2.4.2.5.

To test the viability of the DT concept, it was decided to develop a prototype of the DT platform. The prototype allows to test the feasibility of key payment scenarios as well as assess the risks and limitations associated with the use of distributed ledger technology and token-based access.

Life cycle and dedicated solutions tested in the pilot project



2.1 Review of the DT pilot project

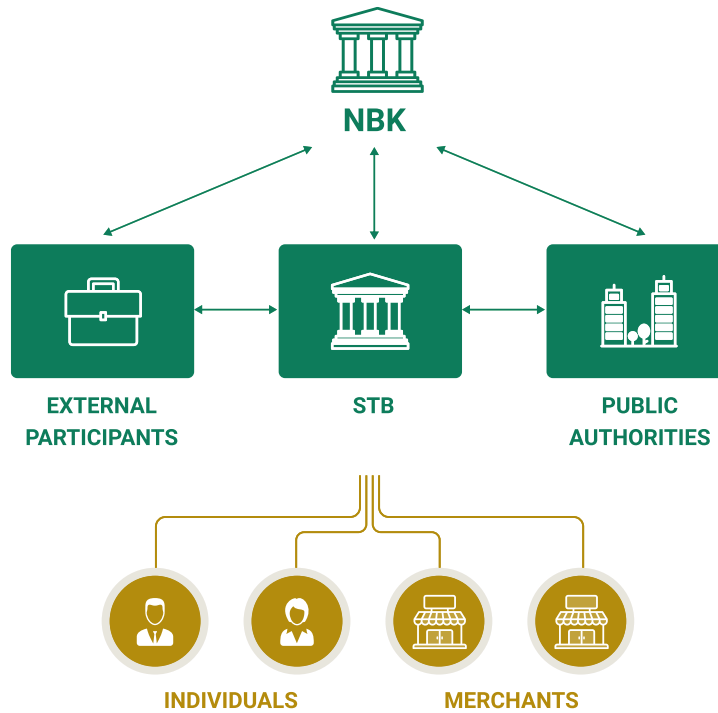
As a result of the pilot project, the following results were achieved:

1. The possibility of implementing a retail CBDC based on DLT technology was experimentally confirmed.
2. Key CBDC life cycle scenarios were developed and tested - from issue to circulation.
3. New potential CBDC's benefits to citizens and commercial organizations were tested, including offline payments, programmability at the token level, the flexibility of the system concerning the balance between transaction anonymity and AML/CFT (customizable anonymity).
4. The connection of second-tier banks and other external participants to the DT infrastructure has been tested (for more details – 2.4.2.9).

2.2 Roles, participants and architecture of the pilot platform

To enable the DT transactions, the pilot platform emulates the following participants that interact with each other under a two-tier architecture:

PARTICIPANTS OF THE PILOT PLATFORM



NBK

NBK is the operator of the pilot platform and ensures the connection of external participants to the pilot platform, monitors platform operations, it is responsible for the issuance, distribution, and redemption of the DT. NBK is the guarantor of the one-time use of tokens and their legitimacy as a means of payment: the notary node of the distributed ledger is located in the infrastructure of the NBK, and its technical function is to check that a token has not been used before. We explain in more detail the role of the notary node under the pilot project scenarios in 2.4.

Second-tier banks (STB)

STBs provide users with digital wallets to make payments with the DT, are responsible for compliance with AML/CFT and KYC requirements, hold and distribute using tokens. STB exchange, redeem, restore the DT and make interbank transfers.

2.2 Roles, participants and architecture of the pilot platform

Public authorities

Public authorities determine a special purpose of tokens, distribute them to end-users, and monitor the intended use of distributed money. Payments are performed via STBs. In the pilot project, only public authorities distribute special purpose tokens.

Merchants

Merchants provide services and goods to individuals, are clients of STBs and open wallets in STBs, and carry out online and offline transactions using tokens (purchase and transfer) with the use of digital wallets.

Individuals

Individuals are citizens who use the platform and interact with merchants, STBs, and external participants. Individuals manage their DT using digital wallets.

External participants

External participants include fintech companies, technology companies, including providers of IoT and other solutions, as well as regulated financial market participants (providers of financial products and services).

External participants connect to the platform and create additional services and products on its basis. The purpose of attracting external participants is to demonstrate the platform's ability to build business applications and implement additional scenarios for creating an ecosystem of the DT services and products. External participants connect to the platform through the integration services of STBs to carry out transactions with the DT and exchange the DT for fiat currency.

Each of the participants in the pilot platform has a specific role:

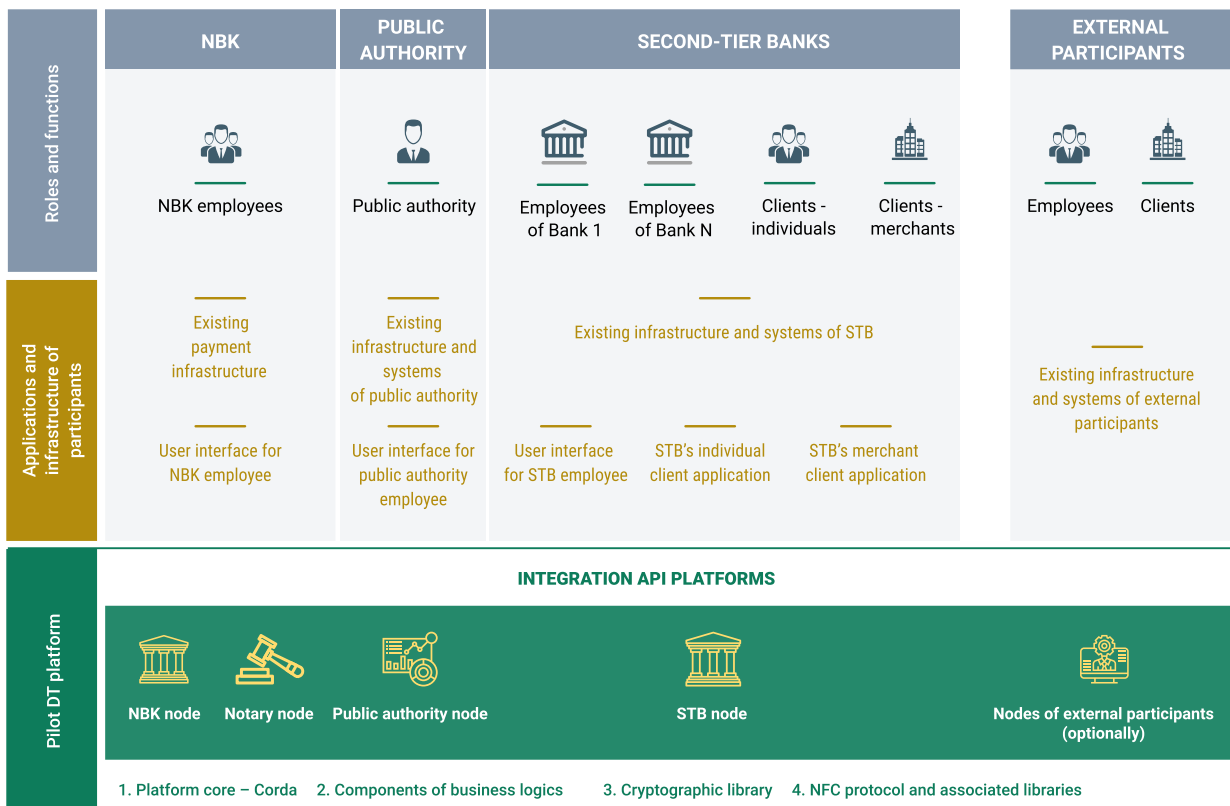
Participant	Platform roles
NBK	Central bank (1st tier)
STB	2 nd tier infrastructure participants
Public authorities	2 nd tier infrastructure participants
Merchants	Users
Individuals	Users
External participants	Ecosystem participants

2.2 Roles, participants and architecture of the pilot platform

In order to test the DT life cycle scenarios in the pilot platform is built on a two-tier DT distribution model, the following roles were emulated:

- Central Bank (1st tier) – nodes in the CBDC network that performs functions such as issuing, redemption, and transfer of tokens.
- Infrastructure participants of the 2nd tier (second-tier banks and public authorities) - nodes in the CBDC network that interact with the 1st tier, hold and distribute tokens themselves. In the pilot project, external scenarios with two STBs were implemented and tested (see section 2.4.2.9). External applications of the STB participants of the pilot project are connected to the pilot platform through the pilot implementation of the API platform.
- Users (individuals and merchants) are end-users who have access to the platform through interfaces of STBs interfaces where they are served. Demo applications for individuals and merchants have been developed in the pilot project.

Pilot platform conceptual architecture



2.3 Choice of technological solution (DLT platform)

To decide on the core of the pilot platform, an analysis of technologies and platforms was made. As a result, the Corda platform, provided by r3, based on the distributed ledger technology, was chosen as a pilot project core.

Key selection criteria:

Criteria	Description
Licensing type	Platform is available in the open-source version
DLT network access control	Permissioned ledger. The opportunity for an organization to control access of new participants to the network
Security and privacy	Opportunity to manage anonymity, confidentiality and traceability of transactions
Flexibility and scalability	Feature to scale-up the platform and maintain a dynamic registry of distributed ledger participants
Performance	Speed of processing and implementation of transactions in the ledger
Interoperability	Support of ISO 20022 and other standards

For future development of an ecosystem of the DT, it is vital to have availability and flexibility for the consensus functionality, the ability to define and manage access rights of participants, as well as the ability to create smart contracts in the ledger [\[8\]](#). The Corda platform provides these capabilities [\[9\]](#).

The initial focus of the r3 on a solution for the financial industry and an emphasis on the privacy of transaction participants is the additional Corda advantage. Additionally, countries such as Sweden, Japan, Canada, Switzerland, South Africa, France, and the European Union already have successful CBDC projects based on Corda.

2.4 Pilot project scenarios

1. Approach to determine a list of tested scenarios

In order to assess the technical feasibility of the pilot platform, it was decided to test assumptions about how the platform should work (hypotheses) using generated practical steps (scenarios).

Prioritized list of scenarios for testing within the pilot project was based on hypotheses, business requirements to the DT properties, international experience in implementing scenarios with CBDC, and technological features.

Correlation of scenarios and tested hypotheses

#	SCENARIO	DESCRIPTION	User friendly access	User friendly transactions	Safe transaction	Lower costs of creation	Lower costs of circulation	Special purpose payments	Program ability	Offline	Analytics
1	Infrastructural participants' wallets creation	Original creation of digital wallets with DT for infrastructural participants	✔								
2	STB clients' wallets creation	Original creation of digital wallets with DT for individuals	✔								
3	Issue of DT	Original creation of DT without transaction history DT issue to created wallets of participants				✔					
4	Distribution of DT	Conduct of DT distribution to end users via STB wallets					✔				✔
5	Special purpose token distribution	Conduct of target token distribution to end users via STB					✔	✔	✔		✔
6	Online transfer	DT transfers between sender and recipient, retail clients of different banks when Internet connection is available to all the participants		✔	✔		✔				
7	Online purchase	Purchase of goods by an individual using DT from a merchant when Internet connection is available to individual and merchant. Individual and merchant are serviced in different banks		✔	✔		✔	✔			
8	Offline purchase	Purchase of goods by an individual using DT from a merchant when Internet connection is not available to individual and merchant. Merchant and individual are serviced in different banks		✔	✔		✔	✔		✔	
9	Scenarios of external participants	Scenarios of external participants with the use of the Pilot Project environment to verify and/or demonstrate technical capabilities	✔								

2. Implemented scenarios

This section describes the scenarios tested on the DT pilot platform.

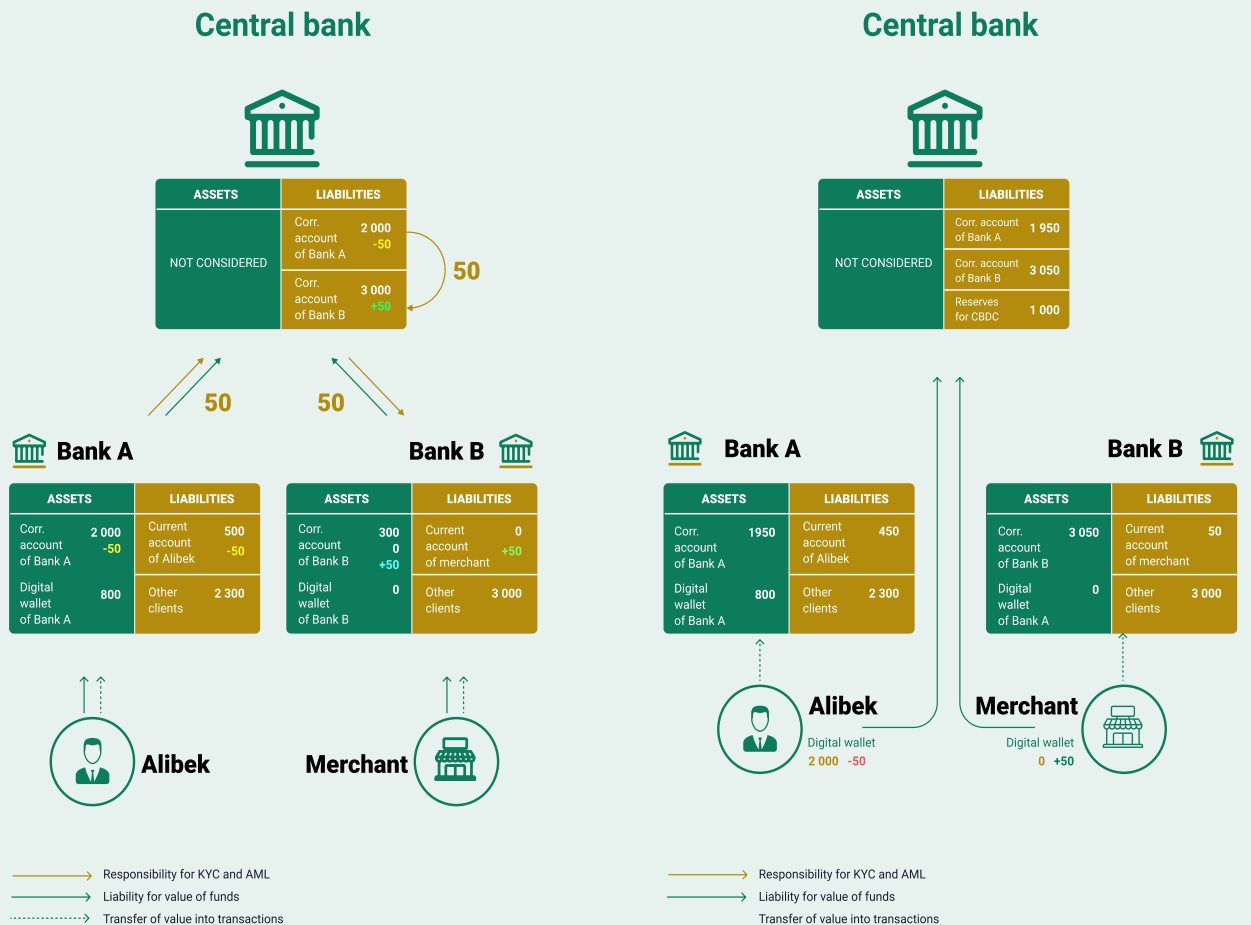
Users control the DT transactions

In existing systems of bank payments, for a client of Bank B to receive money transferred by a client of Bank A, money must go through a multi-stage procedure of mutual settlement.

In terms of the settlement process, transactions on the DT platform are much more efficient: since the DT is represented by tokens, their value can be remitted directly between a sender and a receiver without the need to be reflected in the balances of financial organizations. Even though there is a need to comply with AML requirements and the need to prevent double-spending, verifications by STBs and the notary node of the NBK are preserved, removing the need for clearing and reconciliation. Such a process significantly reduces the time of finalizing the transaction and costs of the parties.

Transaction in RTGS system

Diagram of the online transfer accounting



2.4 Pilot project scenarios

As mentioned previously, the DT uses a two-tier distribution model. It means that NBK distributes the DT tokens to STB digital wallets against their cashless funds. End-users interact with the DT platform via STBs, including connecting to the platform, replenishing wallets, and performing transactions. As part of a pilot project, banks provide these services through their mobile applications.

2.1 Infrastructural participant wallet creation

In order to work with the DT, STBs and other infrastructure participants must connect their nodes to the platform and open wallets that enable transactions with tokens. The possibility to connect new participants to the platform confirms the hypothesis of availability of the DT for STBs and other infrastructure participants:

Easy access - a process of opening a digital wallet of an STB or another infrastructure participant is at least as convenient and safe as the existing mechanism to access payment infrastructure.

On the pilot platform, the process of opening wallets for infrastructural participants, generating their addresses and signatures is implemented with the use of the functionality provided by the Corda platform.

2.2 STB clients' wallets creation

Opening wallets for STB clients is an initial creation of digital wallets for STB clients. The feasibility of opening clients' wallets was tested in the pilot project. As a result, the hypothesis of the convenience of opening a wallet of an STB client was confirmed:

Easy access - as compared to opening accounts in STBs through a mobile application, the process of opening a digital wallet with the DT in STBs is at least equally convenient (it does not include additional effort compared to traditional account opening) and safe.

The DT platform is built on a two-tier model (section 2.2). The onboarding of new users is carried out exclusively through accredited organizations (by the first-tier participant - NBK). Currently, access is piloted according to the 1 to 1 scheme: one wallet is served by one organization.

An individual or a merchant willing to access transactions with DT must have access to the mobile application of one of the second-tier banks. The process of passing primary user identification in banks, (including KYC procedures) is out of the scope of this project.

In STB applications a client can send a request to open a digital wallet. The bank considers the application and confirms the validity of the request. If the application is approved, a set of cryptographic keys is generated on the device of the user. These keys enable transactions on the DT platform: online transfer, online and offline purchases.

Global experience

Possible approaches, including limitations of each of the options, were previously studied by the Central Bank of Sweden in a report covering results of the first stage of the e-krona pilot project [\[21\]](#).

The DT has used an approach where both tokens and keys are stored on a user's device. This allows to smoothly implement an offline purchase process if the connection on the buyer's device is suddenly lost. Unlike approaches where this operation is impossible without first saving part of tokens on the device. Along with that, special mechanisms to store keys of STB clients (see below) must solve the problem described by the Bank of Sweden to user wallets when a user's device is lost.

Keys and signatures

Secret keys for wallets of STB clients were implemented in the platform, which guarantees users the sole control over their money while retaining the STBs capability to track transactions in line with AML/CFT requirements:

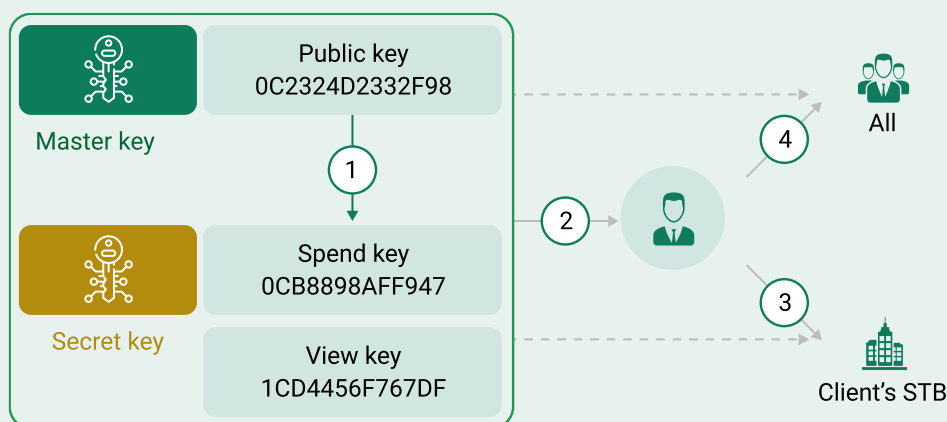
- ✓ Secret key is randomly generated. It is known only to an STB client. After generation, it is divided into two parts:
 - View key – a key providing viewer rights, allowing the user to view the history of transactions made with user tokens. It is stored by an STB and can also be transferred to other organizations with the consent of the user
 - Spend – a key providing spending rights, allowing the user to sign permission to transfer tokens. It is stored only by a wallet owner
- ✓ Public key (publicKey). It is a public address of the STB client's wallet. It is available to the STB client, STB, and other participants. It can be registered in a global register of second-tier banks, for example, to enable the DT transfers between clients by phone number ('The online transfer' scenario is described further in section 2.4.2.6).

2.4 Pilot project scenarios

The key generation diagram is set out in the figure below

1. When opening a user's wallet, a public key is generated on his device. Secret keys are formed from it – Spend key and View key
2. The client has access to all the generated keys
3. View Key is transferred to the STB for compliance with the AML/CFT rules
4. Public Key is the client's identifier to receive payments and it is available to all the network users.

User key generation diagram



2.3 The DT issuance

Issuance is an initial creation of the DT tokens, which are made against STBs reserves in NBK.

The implementation of this scenario is a necessary pre-condition for any other scenarios using the DT and allows to confirm an important hypothesis about advantages of the digital currency:

Reducing costs of creation – secured by obligations of the NBK as compared to cash, the issuance of digital currency can significantly cut associated costs (as well as indirect costs and negative impact on the environment).

2.4 Pilot project scenarios

The Initiator of a request for issuance of the DT can be one of the platform participants - an STB, a public authority, or NBK as part of its monetary functions.

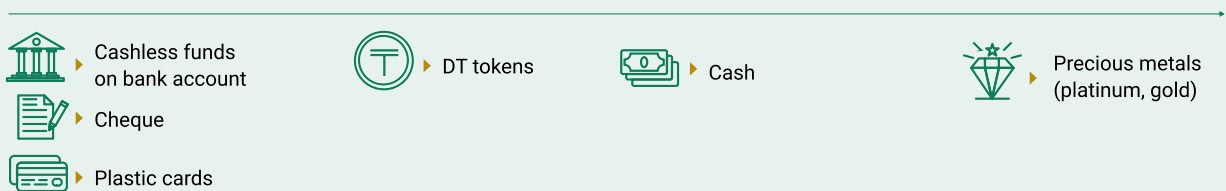
Any token contains information about its issuer - the NBK, which cannot be counterfeited due to the used cryptographic algorithms. This allows all the platform participants to uniquely determine token authenticity. The procedure can be compared to the identification of cash authenticity using analysis of watermarks embedded in their printing.

Token properties

Key properties of the DT token:

- ✓ Value. The token is a representation of a certain value, an amount of tenge indicated in the token
- ✓ Verifiability. The value of a token can be verified based on data available in the token itself.

The property of verifiability can be represented on a scale. At the left corner of the scale are funds that are completely guaranteed by an intermediary: cashless money in a bank account, cheques, and plastic cards. At the right - funds that have an intrinsic value: gold, platinum, etc.



The DT tokens have an intermediate position. They do not replicate all the properties of tangible cash. Along with that, according to the data contained in the token, it is possible to verify the authenticity and value of the token. These properties move the DT token closer to the characteristics of cash assets.

The token structure contains:

- ✓ Encrypted information about previous owners, which allows identifying the issuer of funds - NBK
- ✓ Information about a current owner of DT (in the format of a one-time stealth-address)
- ✓ The DT type (main, social, etc.)
- ✓ Quantity of the DT in a blinded form

2.4 The DT distribution

The DT distribution – a process of transferring the DT from STB to end-users, to a digital wallet (or potentially another token carrier) of the client.

Implementation of this scenario made it possible to confirm the following hypotheses:

- **Reduction of circulation costs:**

As compared to cash: with a distribution of the DT, there are no costs for physical asset transportation and storage for NBK, STB, and public authorities.

As compared to cashless funds: reduction of costs associated with accounting at all levels, since funds in a digital wallet of the client are not recorded on a balance sheet of the financial institution.

- **Analytics** – the capability to collect data related to the DT transactions for market analysis and planning of macroeconomic indicators has been implemented.

A client willing to receive the DT sends a request to his bank. After the bank approves the request, funds are automatically remitted from a digital wallet of the financial institution to the wallet of the client. An important difference from the existing system of cashless payments is the finality of token transfer: funds in the client's wallet, in a manner similar to cash, are not recorded on a balance sheet of the financial institution.

2.5 Distribution of special purpose tokens

Distribution of the special purpose DT – a process of transferring special purpose DT tokens from a government organization to a digital wallet of the client.

The implementation of this scenario made it possible to confirm the following hypotheses:

- **Reduction of circulation costs:**

As compared to cash assets: with the distribution of the DT, there are no costs for transportation and storage for NBK, STB, and public authorities.

As compared to cashless funds: reduction of costs associated with systematic accounting of funds at all levels, since funds in a digital wallet of the client are not recorded on a balance sheet of the financial institution and do not require reconciliations upon accounting.

- **Programmability** – the functionality to limit the spending of funds is provided by type designs of tokens (that is, a capability to embed information about its type into a token, for example, to track its intended use). Changes in information in the structure of the token demonstrate one of the options for the programmability of digital money (also sometimes referred to as 'labeling' the money)
- **Social payments** – the limit on the spending of earmarked funds is achieved by specifics of distribution of these funds, implemented in the pilot project
- **Analytics** – the capability to collect data on the DT transactions for market analysis and planning of macroeconomic indicators has been implemented

Scenario description

The DT programmability feature makes it possible to streamline some existing payment scenarios. For example, a scenario for the distribution of funds for specific purposes.

The DT programmability options

The DT is a programmable means of settlement:

Option 1. It is possible to record token type, owner, or other data in the DT tokens

Option 2. In transactions, the DT operations, you can blind any data of a sender or a receiver, managing the anonymity of transactions

Option 3. At the level of distributed ledger, you can create smart contracts that will be executed when the DT transactions are created.

2.4 Pilot project scenarios

The DT programmability feature makes it possible to streamline some existing payment scenarios. For example, a scenario for the distribution of funds for specific purposes.

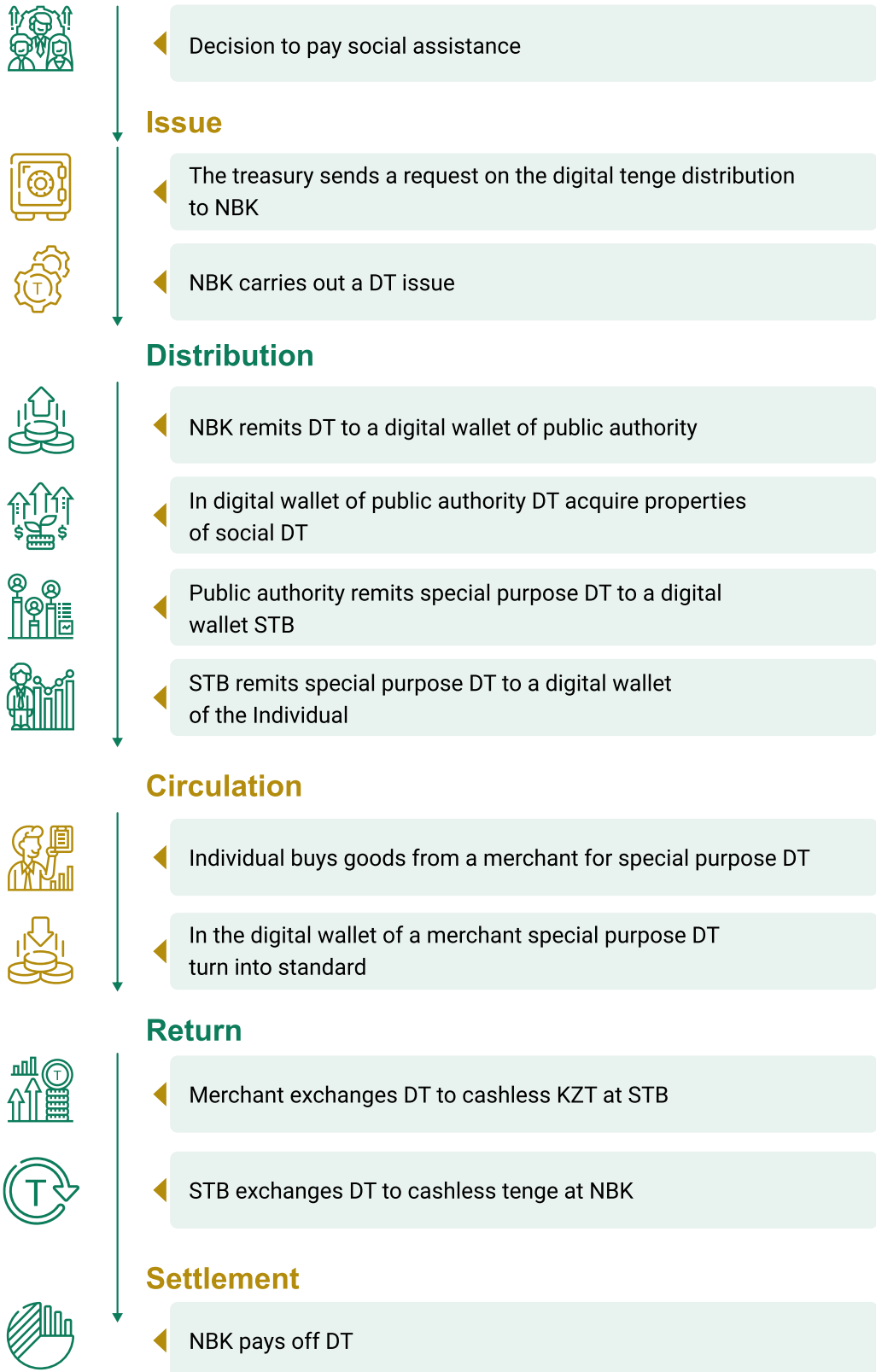
As a confirmation of the programmability of tokens, labeling of tokens and their distribution to STB clients have been implemented on the DT platform.

Tier 1 Bank (NBK) issues the general DT. Then participants with appropriate permissions e.g., some of the government departments can 'label' the DT received from the NBK. The capability to mark issued DT by one of the participants was implemented in the pilot project.

Within the conduct of transactions with a certain type of the DT, it is possible to verify the capability to use the DT in this transaction. For labeled DT, bans on certain transactions can be implemented by NBK, public authorities, or STB. For example, in the pilot project, a ban was imposed for a client to make "Online transfers" of labeled DT. Also, if an attempt is made to pay for a purchase in a store with a special purpose DT, verification can be made that the store can accept labeled DT for payment.

The life cycle of special purpose DT in the pilot platform is represented in the figure below.

Life cycle of special purpose DT on the pilot platform



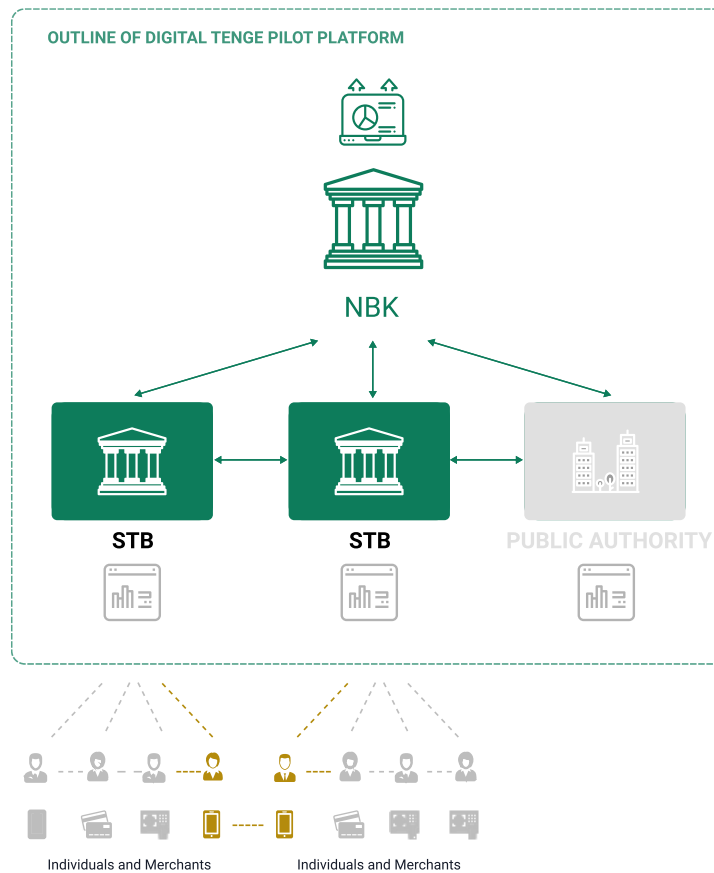
2.6 Online transfer

Online transfer is a transfer of tokens between clients' wallets if both participants have an Internet connection. This scenario reflects the functionality of funds transfer between clients in cashless payment systems.

Tested hypotheses

- Convenience of transactions – the implemented scenario matches the experience of online transfers adopted in cashless payments, allowing to provide at least the same level of convenience for a user.
- Security of transactions - tokens allow for an unambiguous identification of the issuer of funds thus guaranteeing their authenticity. At the same time, a consensus mechanism rules out the double-spending of tokens when an Internet or mobile data connection is available on participants' devices.
- Reduction of circulation costs - transactions on the distributed ledger reduce counterparty risks and functions. That allows reducing transaction costs due to the implementation of direct, risk-free transactions.

Participants of the online transfer scenario



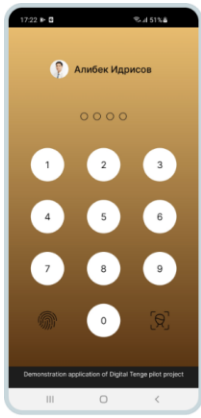
The Scenario as viewed by a user

The process of an online transfer of DT through an STB mobile application is shown in the figure on the next page: for a money transfer, the user just needs to enter a receiver phone number and token amount in the mobile application of the bank. After the transaction is signed by the client and their banks, the DT tokens are transferred from the sender wallet to the digital wallet of the receiver.

At the user level, the procedure seems indistinguishable from present-day solutions for cashless online transfers. However, at the same time, the DT technology does not use mutual settlements between financial institutions – value is transferred directly between customers' digital wallets. This significantly increases efficiency: in the case of traditional centralized systems as cashless payments, a need to clear transactions (and for a card infrastructure a separate cycle of final settlements) is a limitation to finalize settlements.

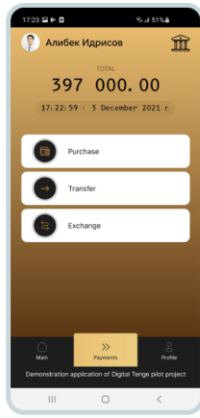
To maintain the advantages of cash, the prototype has tested user-controlled anonymity: the client in settings of his profile can decide for himself whether he wants other transaction parties to see his full name or prefers to blind this data. However, currently, there is no possibility to blind information from the financial institution, since this will not allow them to meet AML/CFT requirements.

Functional description of the online transfer scenario



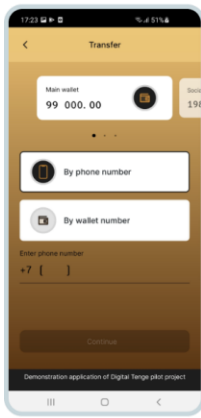
STEP 1

Alibek logs in mobile application of Bank A



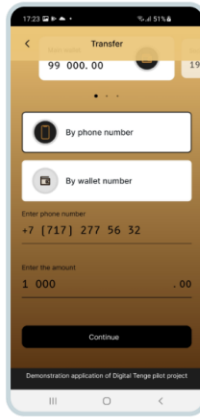
STEP 2

Alibek chooses a wallet from which he will make a transfer: enters phone number of Bakhtiyar



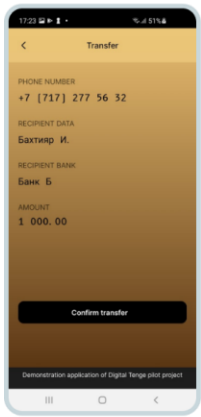
STEP 3

Alibek checks transfer information and signs the transaction



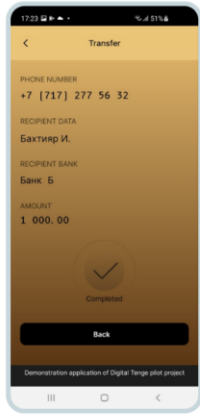
STEP 4

Alibek checks updated balance in the main wallet transactions history



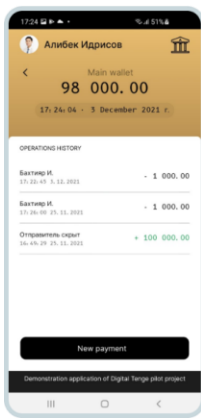
STEP 5

Alibek enters section 'Payments' and chooses 'Transfer' in the menu



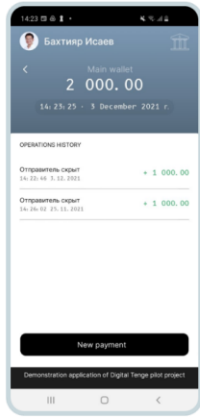
STEP 6

Alibek enters an amount of transfer



STEP 7

Alibek sees transfer confirmation success



STEP 8

Bakhtiyar checks transaction history and sees that money is credited

2.4 Pilot project scenarios

Accounting of funds in settlements

(preliminary approach - it will be further developed at next project stages)

One of the transactions accounting options for the DT platform is shown in the figure below (like cash). Such an approach is possible due to the choice of a token-based model. Funds are **not** accounted for on the balance sheets of financial organizations. This streamlines the existing system of mutual settlements between financial institutions.

Diagram of online transfer accounting

NBK							
Assets				Liabilities			
Not considered				Corr. account of Bank A	1950		
				Corr. account of Bank B	3050		
				DT in circulation (DT reserves)	1000		
Bank A				Alibek			
Assets		Liabilities		Assets		Liabilities	
Corr. acc. Of Bank A	1950	Current account of Alibek	450	Current account of Alibek	450	Not considered	
Digital wallet of Bank A	800	Other clients	2300	Digital wallet of Alibek	200 -50		
Bank B				Bahtiyar			
Assets		Liabilities		Assets		Liabilities	
Corr. acc. Of Bank B	3050	Current account of Bahtiyar	50	Current account of Bahtiyar	50	Not considered	
Digital wallet of Bank B	0	Other clients	3000	Digital wallet of Bahtiyar	0 +50		

Global experience

The token-based model requires that a token stores information about previous owners and transactions. Possible approaches to limit the information available for new token holders were previously studied by the Central Bank of Sweden within the first phase of the e-krona pilot project [22]. The DT pilot project solves this problem through cryptographic mechanisms for blinding user addresses (stealth address) and balances (blinding keys) recorded in the token.

Outward view

Transaction traceability

With the use of his keys and knowing the public address of another participant, the owner of a token can a transaction and sign it. The transaction will be formed according to the rules of the UTXO accounting model, which is close to the one used in cashless transactions. Key properties of this model:

- ✓ transaction has an incoming set of tokens and an outgoing set of tokens
- ✓ the set of incoming tokens of a client's transaction is an outgoing set of tokens from a previous transaction of the client
- ✓ the DT tokens are transferred directly from a remitter to a remitee, therefore, when conducting transactions, they don't cause changes in balance sheets of STB and NBK.

The sense of the transaction that the client initiates and signs can be, for example, as follows:

The owner of 30 KZT from this token is now a member with address a787803.

Any member of the network can view this transaction as well as see the token included in it. From the incoming token, any network participant can also get the public address of the owner, his signature and check that this signature matches the public key.

In the long term, the history of transactions with a specific address can be associated with a specific organization or a customer. Thus, the problem with traceability and de-anonymization of transactions arises.

As a solution, the pilot platform uses one-time stealth addresses which are formed from a secret key and a public key of the sender at the time of a certain transaction. In this case, only the user with a view key can verify that the token belongs to this public address. So, only the user who owns the operational part of the secret key can conduct transactions.

Confidentiality

Due to the use of stealth addresses, the IDs of the participants do not appear in a clear text. However, with a sufficient number of transactions, by analyzing the number of tokens transferred, third parties can de-anonymize the participants and obtain information about the number of the DT that the participants have left as a result of transactions.

Corda provides token a re-issuance functionality to 'break' history and solve such a problem. However, in our opinion, this is only a partial solution, since breaking the history even after each transaction does not prevent leakage of information about the balance of the remitter [\[22\]](#).

On the pilot platform, transaction inputs and outputs are modified with homomorphic cryptographic obligations to blind user balances [\[4,5\]](#). Thus, the token owner blinds the number of the DT in it from external participants, while other participants can check the validity of transactions.

When the receiver has no Internet

The problem associated with the use of cryptographic obligations is that for its formation, both participants (both the sender and the receiver) must exchange the results of some calculations using their secret keys. In general, the receiver of the transfer must be online all the time to be able to receive the DT.

Client - the receiver can sometimes be offline. Meanwhile, we suppose that STB is always online. That is why the obligation of a client's incoming transactions signing can be transferred to the client's bank. Thus, the roles of a 'holder' of tokens (STB of the client) and an 'owner' of tokens (client) are separated.

To implement separation of functions of a 'holder' of tokens and its 'owners', the secret key can be divided into 2 parts, one of which will be used by the bank when processing incoming transactions through a wallet of the client.

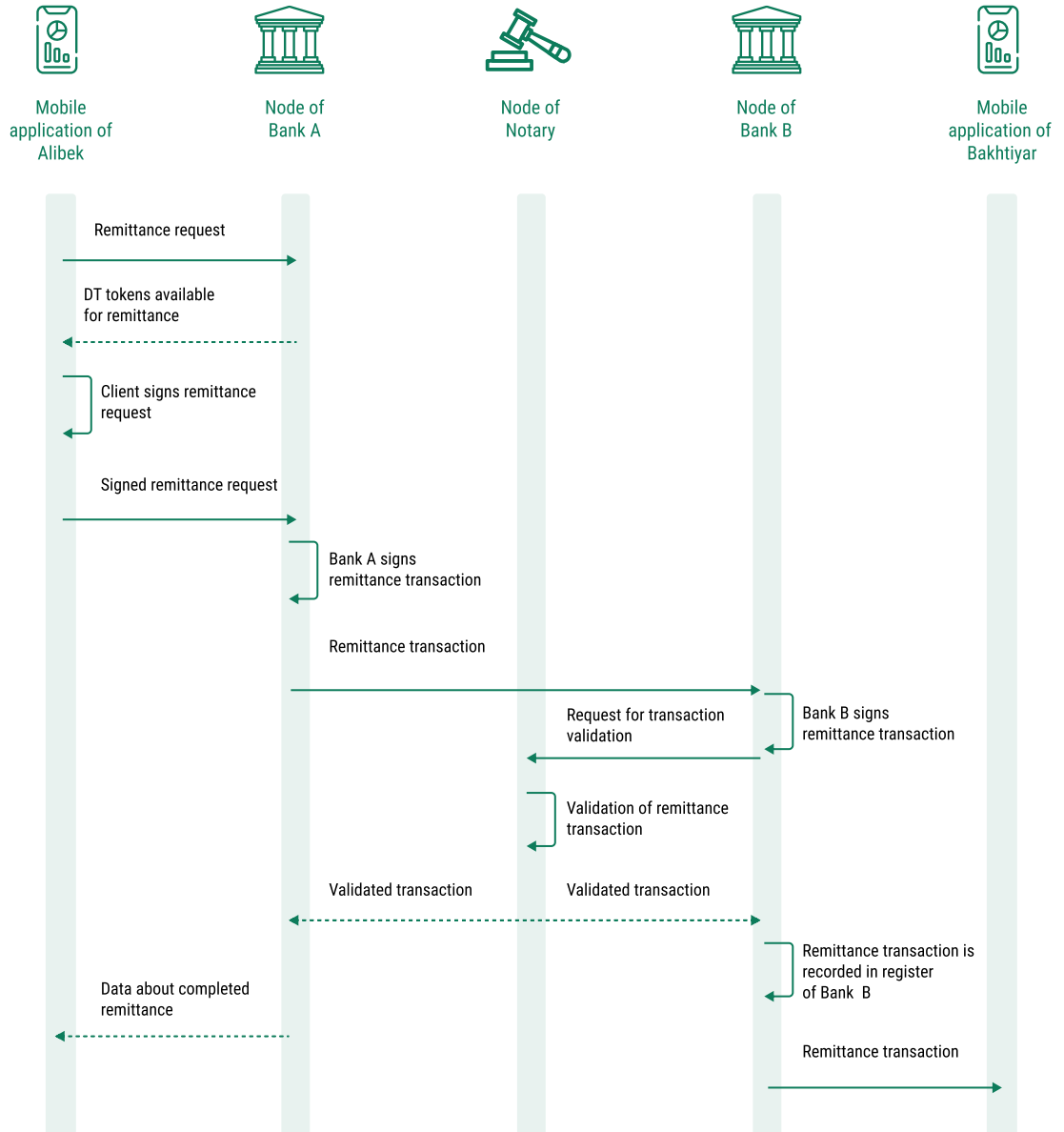
In the pilot project, blinding keys are used for this purpose. Blinding keys are one-time keys that blind the number of the DT in the token and are created for each token in a new transaction. With the help of such keys, the STB can participate in the exchange to form a correct cryptographic obligation, but it cannot form new transactions or change an amount and a recipient in the transaction without the participation of the client (the DT owner and his secret keys to prove ownership of the token - secretKey and viewKey).

2.4 Pilot project scenarios

Additionally, to a sender and a receiver, their banks and the NBK notary node participate in a transaction. The Notary node verifies the uniqueness of tokens checking that they were not spent earlier.

Banks act as guarantors of the legality of transactions. Implemented several types of keys allows a user to retain full control over his tokens. To limit the information available to other participants, cryptographic mechanisms were implemented.

Interaction inside the platform – online transfer



2.4 Pilot project scenarios

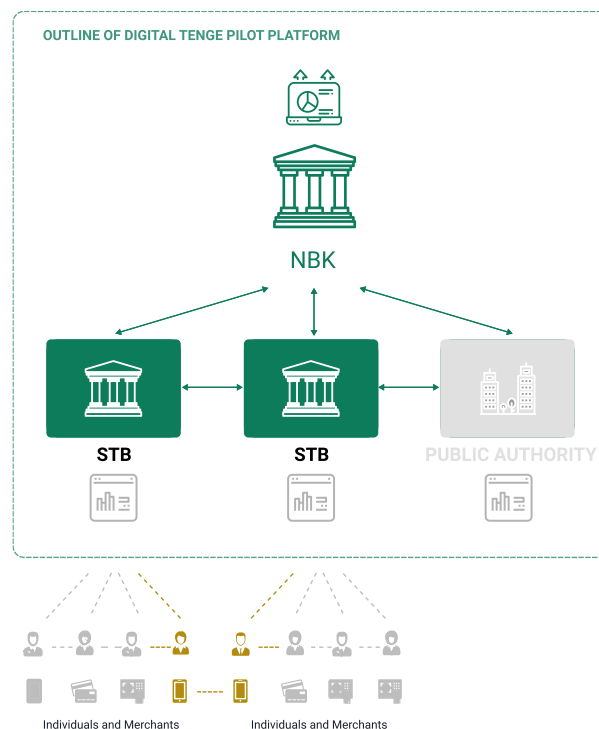
2.7 Online purchase

The online purchase represents a transfer of tokens between digital mobile wallets of an individual and a merchant if at least one of the participants has an Internet connection. User devices must be within the range of an NFC connection or a similar near-field communication protocol during the transactions.

Tested hypotheses

- **Convenience of transactions** - the implemented scenario matches the existing experience of cashless purchase, allowing to provide at least the same level of convenience for a user.
- **Security of transactions** - tokens allow to unambiguously identify a funds issuer, guaranteeing their authenticity. At the same time, a consensus mechanism rules out the possibility of tokens' double spending when an Internet connection is available on the devices of the participants.
- **Reduction of circulation costs** – DT allows transactions with risk-free central bank money. Due to the use of a token-based model, the final settlement happens at the time of the transaction. It allows reducing settlement time and intermediary fees.
- **Social payments** – special-purpose tokens can be used for online purchases. The feasibility to limit purchases with special-purpose tokens accordingly to merchant type is implemented. The approach is described in section 2.4.2.5

Participants of the online purchase scenario



The scenario as viewed by a user

The process of online purchase as implemented on the pilot platform is shown in the figure on the next page. For the user convenience, process mechanics rests on the experience of cashless payments: merchant cashier generates an order in its mobile App, selects the DT as a payment method, and asks a client to bring closer his device. The buyer logs in to the application of his bank and selects a digital wallet from which tokens will be debited. When the devices are brought together, transaction data is exchanged, and the DT is transferred to a merchant account.

Please note that payment in this case (see figure below) was made from a social wallet. This is a wallet to work with type-designed DT, the use of which can be restricted at certain merchants. This functionality is possible due to the programmability of the token, and it is not currently found in other open payment systems.

Functional description of the online purchase scenario

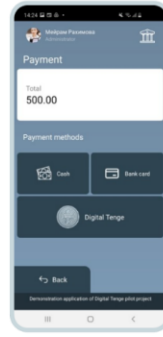
STEP 0

Alibek makes an order in a café and says that he will pay with DT.



STEP 1

Cashier enters an order: picks goods from a menu



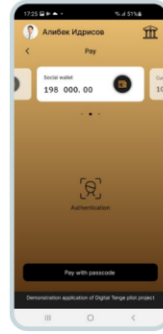
STEP 2

Cashier adds the order to a cheque. Then the cashier switches to the menu 'Payment' and selects payment method: DT



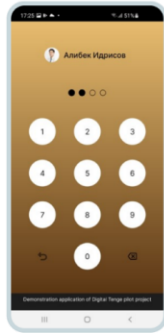
STEP 3

Cashier asks Alibek to bring his mobile device closer for payment



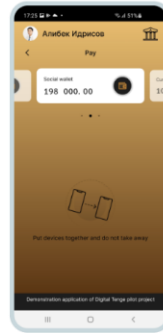
STEP 4

Alibek enters application of Bank A, clicks 'Buy', picks social wallet



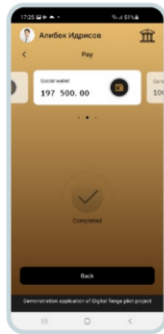
STEP 5

Alibek confirms payment via authentication



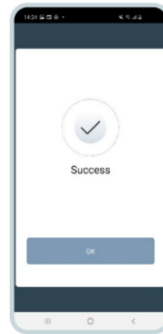
STEP 6

Alibek brings his telephone to cashier's mobile device



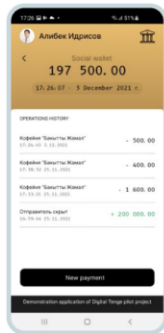
STEP 7

Alibek sees confirmation of the payment and updated balance of social wallet



STEP 8

Cashier's mobile device displays information about successful sale



STEP 9

Alibek checks transaction history of social wallet that his money are debited



STEP 10

Cashier switches to the reports section where the purchase is displayed

Outward view

Token transfer methods

To enable the tokens transfer, it is necessary to provide for a possibility of two-way exchange between two devices taking into account all the employed architectural solutions (in particular, mechanisms of secret keys and balance blinding).

Three main data exchange technologies that meet this requirement:

- Wi-Fi direct [\[3\]](#)
- Bluetooth [\[3\]](#)
- Near Field Communications (NFC) [\[1,2\]](#).

In order to test the technological hypotheses in the pilot project, a decision was made to employ the NFC protocol and implement mobile applications with the functionality of offline purchases on Android OS. This choice among other possible implementation options was justified by the following factors:

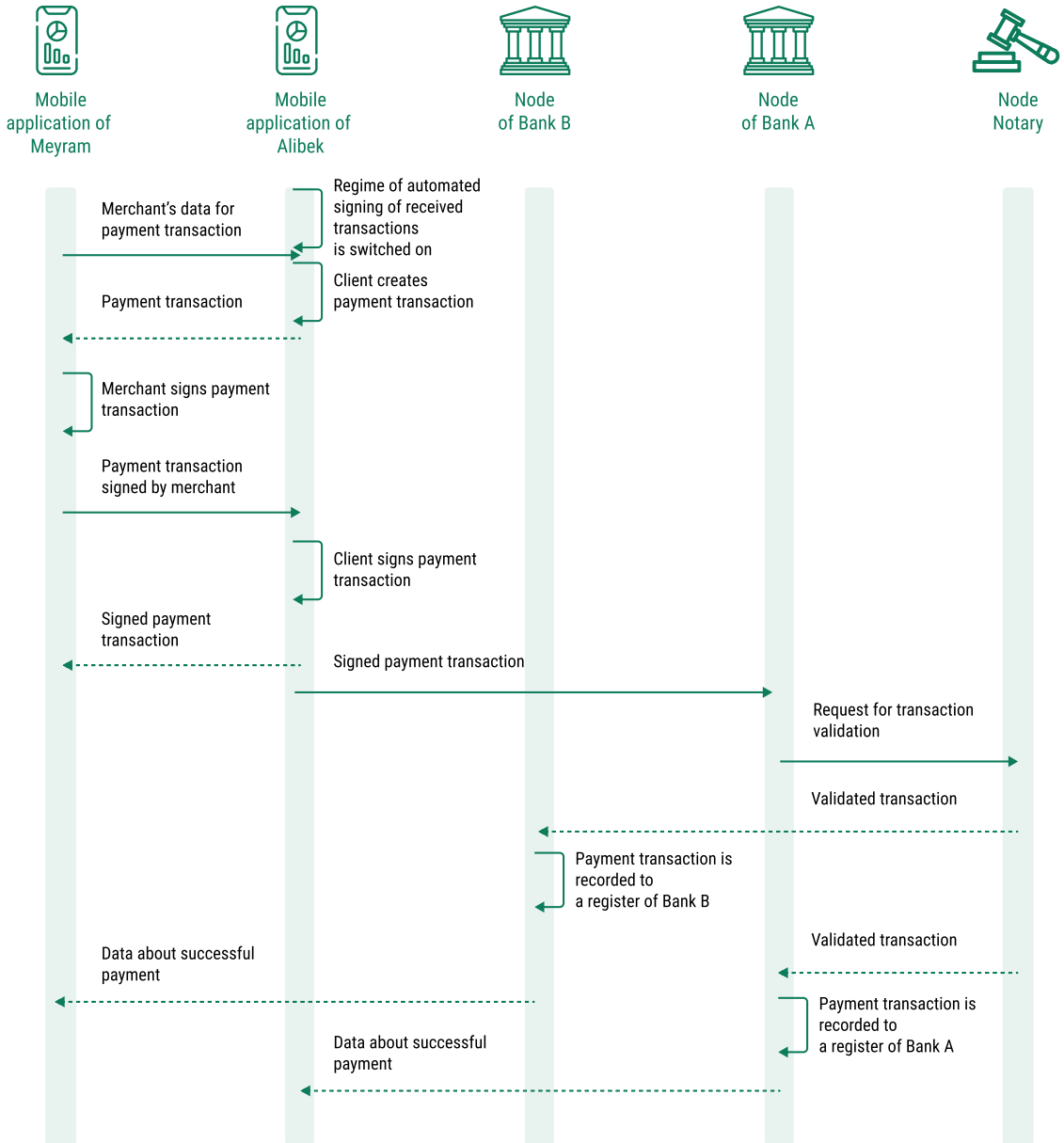
- NFC applications for purchases is native for users who use Apple Pay and Google Pay
- The implementation of transfers and interactive communication via NFC for Android is a more researched topic compared to the exchange via NFC for iOS.

The technical difference between the online purchase process and online transfer is a need to form a transaction template and direct two-way exchange of payment data between participants' devices.

Although the scenario of a payment for an online purchase has long been successfully used for cashless payments (MPS cards, ApplePay, SamsungPay, etc.), when implementing such transactions on the DLT platform of the DT, a challenge arises associated with an increase in the number of streams and data volume that transferred between participants devices.

2.4 Pilot project scenarios

Interaction inside platform – online purchase



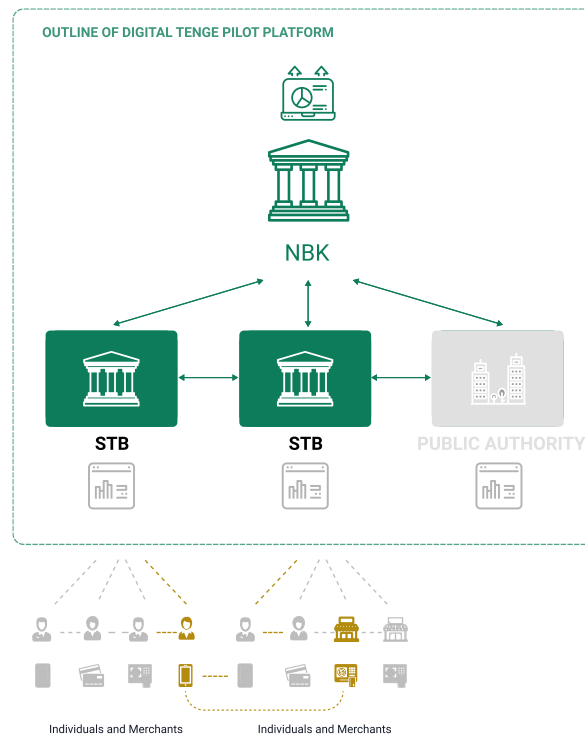
2.8 Offline purchase

The offline purchase is a transfer of tokens between the digital mobile wallets of an individual and a merchant if an internet connection is unavailable to both participants. User devices must be within the range of an NFC connection or a similar near-field communication protocol during the transaction.

Tested hypotheses

- **Offline payments** – the pilot platform includes a capability to make a purchase – the DT transfer between two devices with digital wallets when Internet access is unavailable to both settlement participants (within the current PoC, a one-time purchase / offline transaction was tested without reusing tokens offline).
- **Convenience of transactions** - the implemented scenario matches the existing payments experience of cashless purchases, allowing to provide at least the same level of convenience for a user. At the same time, it becomes possible to make digital transactions in regions without an internet connection. Such a scenario was previously only possible for cash payments.
- **Security of transactions** - tokens allow to unambiguously identify an issuer of funds even offline. However, for production-ready implementation, it is necessary to provide mechanisms to mitigate risks of double-spending.
- **Reduction of circulation costs** – the functionality of offline payments will increase the share of cash turnover and, as a result, cut costs and mitigate risks associated with cash transactions.
- **Social payments** – a capability of purchases with special-purpose tokens has also been implemented for offline payments. The approach to limit spending by special purpose tokens (see section 2.4.2.5) also works when the Internet connection is completely unavailable.

Participants of the offline purchase scenario



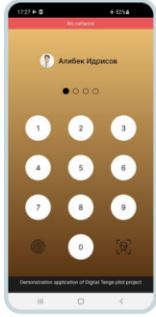
The scenario as viewed by a user

One of the most important properties of cash is that transactions with it can be made when an Internet connection between a sender and a receiver is unavailable. The need for an internet connection is one of the limitations of electronic payments. Since the DT platform uses a token-based model, theoretically, it is possible to carry out transactions with the DT when an Internet connection between a sender and a receiver is unavailable.

To test this assumption in practice, the following configuration of the offline purchase scenario was implemented in the pilot project: the merchants can accept funds from a buyer offline, but their further use requires synchronization of these funds online. Due to the technical specifics of the UTXO model (see 'The online transfer scenario'), this limitation is also imposed on buyer funds received as a change. Despite this, it is a useful scenario when an Internet connection is unavailable to users for a short period.

In the future, it is planned to analyze more complex offline payment scenarios, including several consecutive offline transactions and an introduction of restrictions to mitigate associated risks.

Functional description of offline purchase scenario



STEP 0

Alibek makes an order in a café and says that he will pay with DT. Alibek has no Internet connection



STEP 1

Cashier enters an order: picks goods from a menu



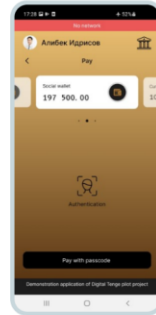
STEP 2

Cashier adds the order to a cheque. Then the cashier switches to the menu 'Payment' and selects payment method: DT



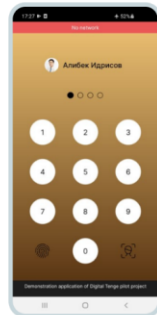
STEP 3

Cashier asks Alibek to bring his mobile device closer for payment. Till is offline



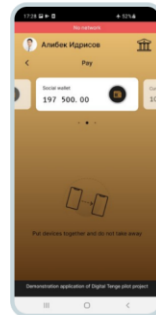
STEP 4

Alibek enters application of Bank A, clicks 'Buy', picks social wallet



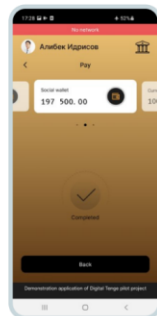
STEP 5

Alibek confirms payment authorization via authentication



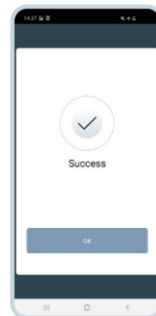
STEP 6

Alibek brings his telephone to cashier's mobile device



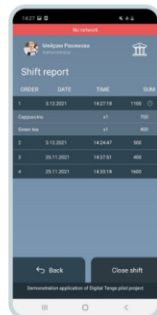
STEP 7

Alibek sees confirmation of the payment and updated balance of social wallet



STEP 8

Cashier's mobile device displays information about successful sale



STEP 9

Cashier goes to report section which displays that sale transaction awaiting synchronization



STEP 10

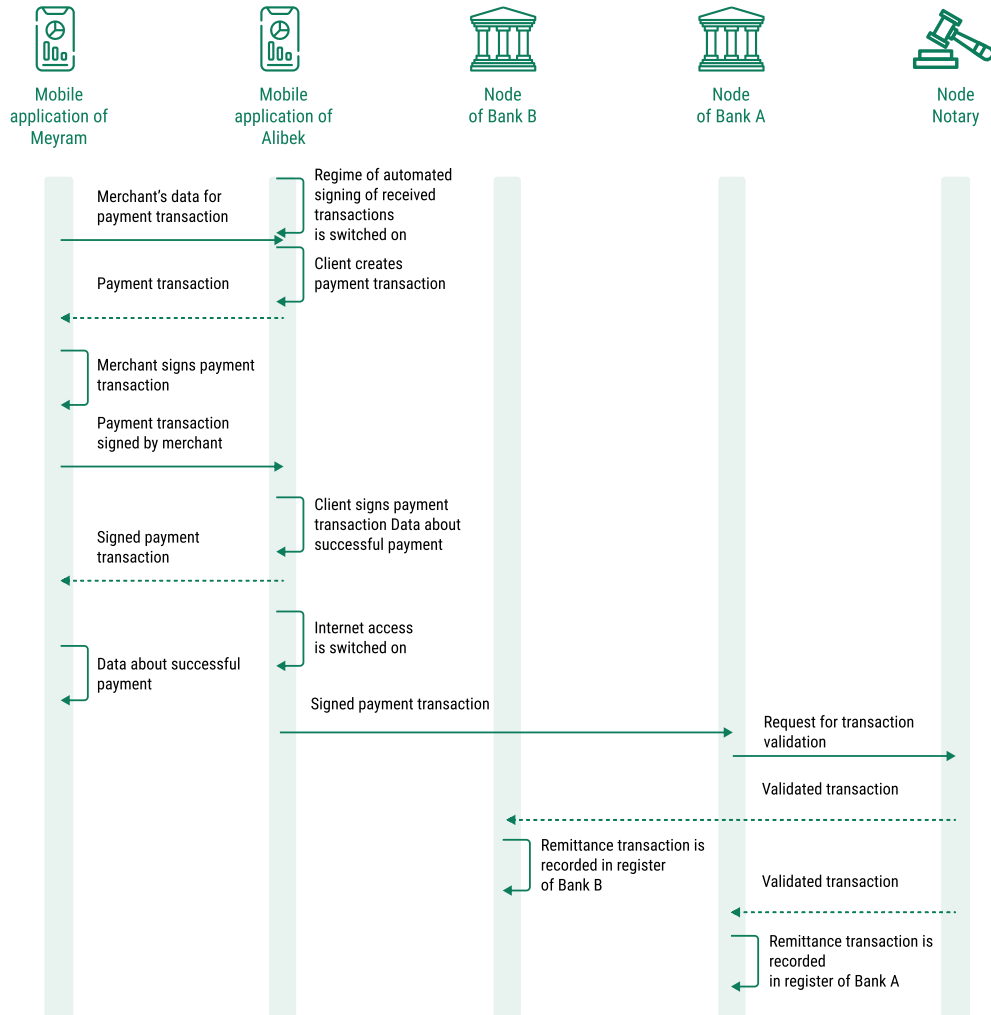
Cashier's mobile device gets connected to the Internet: transaction is synchronized

2.4 Pilot project scenarios

Outward view

The process reflecting the offline purchase in the figure below does not differ much from the process reflecting the online purchase. However, after a transaction between the seller and the buyer, at least one of them must go online to finalize payment. During the synchronization, tokens are verified, and the transaction is recorded to the ledger.

Interaction within the platform – offline purchase



Risks and challenges for offline payments

The token-based model allows to implement of reliable mechanisms of risks limitations for participants before token synchronization:

- ✓ Information about the issuer is cryptographically embedded in the token structure. It cannot be changed, and it is transferred along with it. This eliminates the risk of counterfeited funds.
- ✓ Each token is unique and keeps a history of all the transactions made with it. That is, after tokens synchronization by at least one of the payment parities, participants that made suspicious transactions can be unambiguously identified through KYC data.

Technical solution restrictions

In order to rule out the risk of multiple uses of the DT tokens, a consensus mechanism is provided. This algorithm is implemented using a notary node and smart contracts that determine what operations can be performed with tokens. Smart contract scripts can automatically verify compliance with basic restrictions on the DT operations, for example:

1. The transaction with the DT from a token was approved by a token owner. For this, the transaction must be signed by the token owner.
2. The owner of a token with the DT is an organization or an individual that has passed the KYC procedures with the STB. To ensure this, the transaction must be signed by the STB serving the client.
3. During the transaction, the total number of the DTs transferred did not change. To ensure this, the notary node verifies checksums of inputs and outputs of the transaction.

In online mode, when an attempt is made to transfer a token that has already been used, the notary node will block the transaction.

However, **in offline scenarios** when external participants are unavailable, the problem of possible multiple spending DT remains, therefore, to protect the interests of the recipient, administrative measures must be provided to influence the owners who perform fraudulent activities with the DT.

2.9 Scenarios of external participants

Scenarios with external participants were also implemented in the pilot project. During the scenarios' implementation, the feasibility to connect and interact with the existing participants of the financial market with the DT pilot platform was tested.

As a result of an open invitation for STBs to participate in the pilot project, several banks have demonstrated their readiness to join the project in a short time and implement their scenarios using the DT, building integration with the pilot platform via API in a test environment. Scenarios for implementation were offered by external participants and tested the advantages of the DT for STBs.

During the development of the scenarios, first, a technical capability of connecting external participants to the pilot platform was tested, which served as a confirmation of the hypothesis:

Easy Access – a mechanism to connect external participants is fast and simple. Test results have demonstrated that the timing, resources, and costs of connecting external participants to the Platform are adequate.

Approach to selection of external participants

In June-July 2021, NBK held a series of meetings with market players, where it invited banks and fintech companies to participate in the pilot project. Key requirements included:

- ✓ Experienced team with technological expertise (DLT Apps, Dapps / Open API / IoT, SDK, REST, GraphQL, JWT, Mobile / Web Development)
- ✓ Availability of managerial and product competencies; The competencies must be confirmed by sold products
- ✓ Willingness to quickly mobilize the team for design and development, providing its availability for daily communication, and willingness to work within Agile methodology;
- ✓ Availability of its own IT infrastructure, applications, and specialists for project implementation

Candidates were selected in several stages:

1. At the first stage, a selection was made among the participants who applied and complied with the above criteria
2. Further, scenarios offered by the banks for implementation within the pilot project were evaluated. Scenarios must demonstrate the functionality of the DT platform
3. At the final stage, time, labor costs, and API required to implement the scenario were estimated.

2.4 Pilot project scenarios

Following the results of the selection, two STBs have joined the project and successfully implemented their scenarios:

Kaspi Bank JSC (with the involvement of Kaspi Pay team) and Eurasian Bank JSC.

Within the project, together with external participants (STBs), two scenarios were implemented:

- ✓ **Scenario 'Loan repayment using the DT.'** The capability and convenience of integration with existing banking products are important factors when working out the issue of introducing digital currency in the Republic of Kazakhstan. The implementation of the scenario allows expanding the range of the DT application and test functionality that is important both for the bank's clients and for the second-tier banks themselves. For the scenario, an STB working group has updated a test version To work with the DT, additional interfaces and integration with the pilot platform were implemented in the mobile application.
- ✓ **Scenario 'online transfer on the DT platform'.** Currently, an online transfer is one of the most frequently used banking operations by customers. Therefore, this scenario must be simple and intuitively familiar to users and future owners of the DT. To test this feasibility offline transfer between STB clients was implemented within the pilot project. For this scenario, integration with the DT platform was performed on the STB side.

An additional external scenario was developed and tested by an internal team of the pilot project. The scenario includes integration with external applications:

- ✓ **Scenario 'The usage of special purpose tokens to pay for medical services.'** The purpose of the scenario is to test the capability of special-purpose tenge usage when paying for services. The use of special-purpose tokens makes it possible to increase the transparency of payments when paying for goods and services, including the use of public funding. As part of the scenario, integration of the DT platform with specially developed test applications of a medical organization and a social fund was implemented.

Technological aspects of external participants connection

External participants can connect to the pilot project software after completing a registration procedure.

NBK determines the procedure for the participants' registration on the platform and monitors their actions in the distributed ledger. Also, the actions of participants in the ledger are monitored with the use of the notary node, which validates and verifies all the transactions.

During the pilot project, the feasibility of dynamically connecting the registry of the participants was studied. This functionality was taken into account in the architecture of the pilot platform, and it can be implemented using a toolkit of the Corda.

The interaction of external participants with the pilot platform was implemented through an API. The developed interfaces provide an opportunity to:

- ✓ Open and register wallets of STB clients
- ✓ Distribute the DT from STBs to STB clients
- ✓ Carry out transactions:

From STB clients to an STB wallet (from a client of the participant directly to the participant). An example of such a transaction is shown in the figure below;

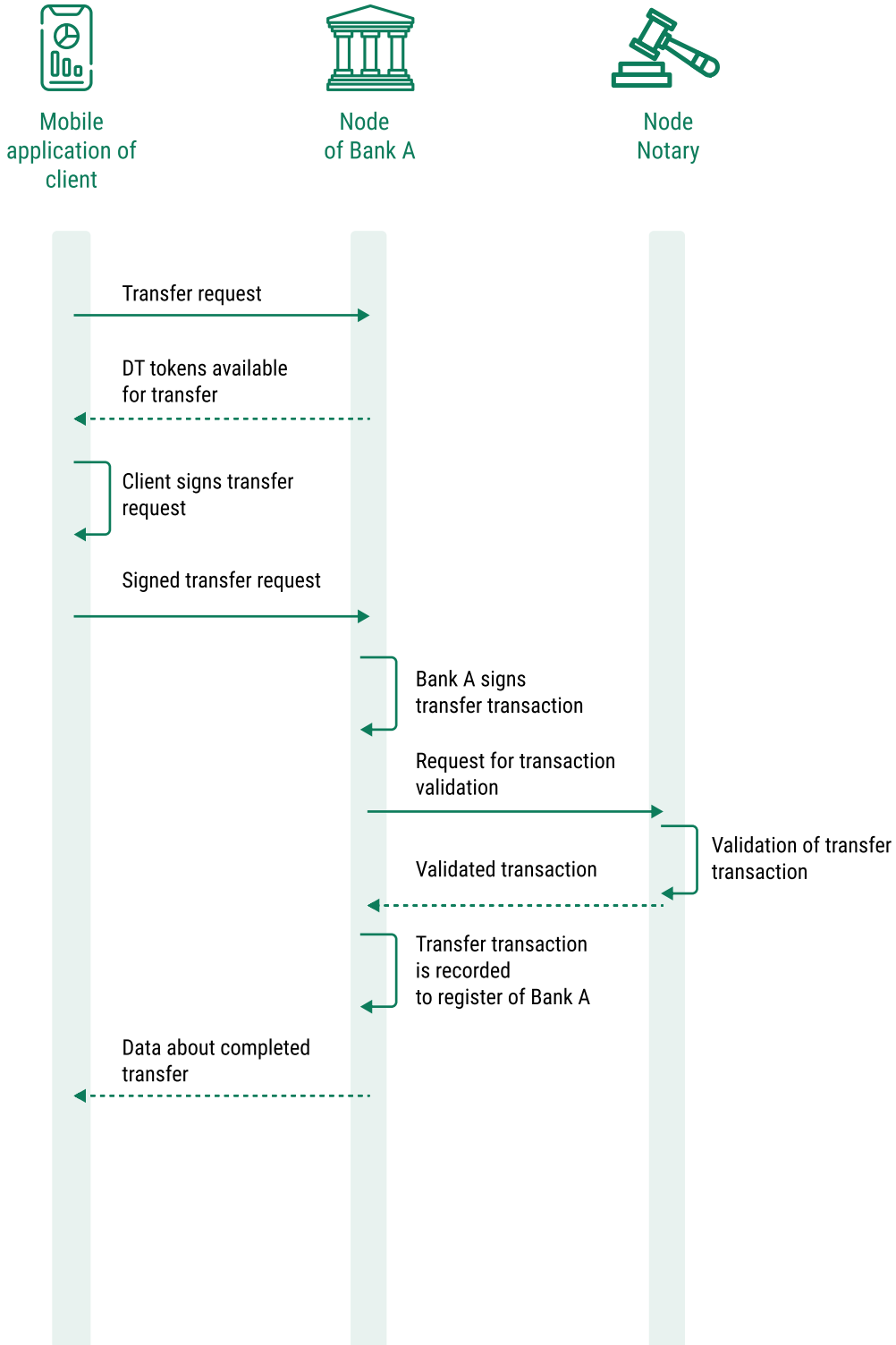
From STB 1 to STB 2 (between nodes of different participants);

From STB clients to STB clients (inside the node of one of the participants). An example of this interaction is given in section 2.4.2.6 below.

On further stages, the way external participants interact with the platform will be the Corda itself, which provides security measures and controllability of the transactions performed.

2.4 Pilot project scenarios

Example of a transaction of transfer from STB client to STB



2.5 Technical aspects for further elaboration

Key issues that should be addressed further are the technical aspects associated with the DT functionality implementation.

1. Offline transactions transfer method

The offline purchase scenario requires a two-way exchange between devices (see section 2.4.2.8). Therefore, we considered only those methods that allow the bilateral exchange. As we mentioned earlier (see 2.4.2.7), the NFC protocol on Android devices was used as an exchange technology in the pilot project. These two factors (protocol and OS types) are the initial limitations of the pilot project. With further study of offline transactions, it is necessary to research the possibility of using the implemented algorithms for devices with other operating systems (in particular, iOS). Additionally, in further development, it is crucial to analyze the possible limitations of the implemented algorithms when scaling the solution.

2. KYC procedures for STB

STBs store information about their clients, sign transactions of their clients, and can identify their clients in a transaction with the use of the spend key associated with the client's wallet.

The accumulation of transactions data at an STB (for all clients or that STB) requires a potential adjustment and increased capacity within the existing infrastructure of STB.

During the pilot project, the analysis of the amount of information that can be generated over a certain period was not performed. This issue requires additional exploration with the involvement of STBs since the amount of stored data also depends on transaction parameters and customer data, which can be specified by participants as mandatory for customer identification procedures.

3. Offline transaction chains

When a user makes a transfer or payment online, the notary node verifies a transaction. Then it is recorded in the ledgers of the participants who participated in the transaction. For example, a client of bank A made an online payment using a mobile device at a merchant, which is serviced by bank B. The online payment transaction will be saved in ledgers of banks A and B. Therefore, when the client of bank B makes a transfer to the client of bank A, the history of Bank A's customer transactions will be consistent and correct.

2.5 Technical aspects for further elaboration

If a client of bank A makes a payment at a merchant, which is the client of bank B, using a device outside the Internet access zone, synchronization and recording of transactions in ledgers of banks A and B will take place only after the device access the Internet. For example, the following situation may occur:

1. Client of bank A pays offline for purchase at a merchant of bank B;
2. Client of bank B remits offline to a client of bank A some quantity of the DT;
3. Client of bank A pays offline for another purchase at a merchant of bank B.

A chain of offline transactions will be saved on a mobile device of the client of bank A. And when his mobile device gains access to the Internet, the chain will be added to the transaction history in the registry.

Transactions related to the client's wallet must be chained, where transactions' hashes are used as links between the records. After performing an offline transaction, the information about the created operations must be embedded in the cyclic graph of the client transactions, which is built based on transactions between his wallet and nodes of other participants. The more offline transactions a client performs, the more complicated the validation and synchronization of transactions will be.

To follow AML/CFT requirements, STBs sign clients' transactions online. When a client receives tokens offline, the bank is not involved in the process of signing and verifying the operation upon the AML/CFT requirements. Therefore, in the prevailing case, the client will not be able to use the DT tokens received offline. To use tokens received in the offline transaction, the client must be able to conduct a transaction without the involvement of STBs, which can afterward be recorded in a distributed ledger after synchronization. The options to implement such functionality also require further elaboration at the next stages.

4. Light clients of the platform

In theory, clients can conduct transactions without a signature from STBs. To do this, light versions of the core platform can be used. At the time of the pilot project development, Corda did not implement a library for the client's signing of transactions without the bank's involvement. Therefore, the scenario of using the DT tokens received offline before the synchronization with the distributed ledger was not verified during the pilot project.

If the core of the pilot platform enables a client to completely sign transactions offline, the client will be able to use the DT tokens right after he receives them offline. Along with that, the need for synchronization remains to comply with AML/CFT requirements and to solve problems of double-spending of the received DT tokens.

The possibility of using light clients requires additional exploration both from the technical side (after implementation of the signature option on the side of Corda r3) and from the administrative side to develop AML/CFT measures and suppress fraud.

5. Scalability

The scalability of the pilot platform is a significant aspect to be taken into consideration during the design and development of the DT platform. Possible directions to analyze the scalability of the solution are 1) architecture of participants' nodes (including the ability to replicate and parallelize parts of the ledger and load balancing); 2) use of off-chain transactions to reduce DLT load [\[10\]](#).

At the same time, further analysis of the scalability and extensibility of the solution must be carried out regarding a chosen platform core. Previously, some studies covered the scalability analysis of r3 Corda, such as a joint study of the possibility of US stocks post-trading processing on a distributed ledger basis. Results presented by DTCC, Accenture, Digital Asset, and r3 have demonstrated that Corda may conduct over 100 million transactions daily [\[11\]](#). We have also found that 'throughput efficiency' (a maximum number of requests for a period of time) of the ledger with 4 Corda nodes, may support 300 transactions per second [\[12, 13\]](#).

To assess the scalability of the DT platform, it is necessary to conduct experiments taking into account specifics of the target architecture, including:

- nature of the interaction between the participants during various scenarios (multistage and sequence of interaction)
- structure of transactions of different types
- number and architecture of node-participants of the distributed ledger
- features of platform infrastructure
- the forecasted number of DT users.

2.5 Technical aspects for further elaboration

6. Open-ended questions

Taking into account the above-mentioned key technical aspects, the following pivotal issues (for which a solution has yet to be found) for the introduction of the DT are:

Key pivotal issues and aspects for further elaboration

Description	Summary	Solution for the pilot and aspects of further elaboration
Centralized wallets vs decentralized wallets	<p>Options:</p> <ol style="list-style-type: none"> 1) Different wallets in different banks according to the two-tier model 2) NBK manages a single wallet and second-tier banks only open wallets 	<p>The pilot project provides a two-tier model: STBs open and serve clients' wallets, NBK issues the DT and manages participants.</p> <p>Using this model in the long term, it may be relevant to implement a 'single window' for management of the clients' wallet (using Open API for data access and transactions initialization) or provide flexibility in the sub-wallets creation.</p>
Anonymity / confidentiality vs transparency and AML/CFT	<p>Preservation of cash properties implies the possibility of anonymity/opacity of transactions for others. At the same time, subject to AML/CFT requirements, STBs must be able to identify, track and store transactions of their clients.</p>	<p>'Customizable anonymity' solution has been offered: only STBs serving clients have access to their client's transactions. At the same time, information about payment participants is not available to external parties. Users can choose whether to show personal data to other users involved in the transaction.</p> <p>The issue of transactions traceability in the distributed ledger of the NBK as well as the regulation of this process requires further study in terms of both regulatory and engineering aspects.</p>
NFC vs other offline technologies	<p>A two-way exchange between two devices is possible with the use of different technologies, including:</p> <ul style="list-style-type: none"> ▪ NFC ▪ Wi-Fi direct ▪ Bluetooth ▪ and other methods of exchange 	<p>The pilot project has applied NFC for offline purchases. With further implementation, alternative solutions can be additionally investigated (both from the point of view of consumer experience and technological feasibility), which will make it possible to decide which data exchange technology will be used.</p>

2.5 Technical aspects for further elaboration

Description	Summary	Solution for the pilot and aspects of further elaboration
Offline time vs double spending risk	Users can make purchases when the Internet is unavailable to both the client and the seller but at the same time there is a risk of double-spending (the risk that in a complex technological attack, a transaction with tokens that have already been spent can be carried out)	The pilot project has implemented and tested just the functionality of offline payments; there was no detailed study of mechanisms to mitigate risks of double-spending. To implement an industrial solution, it is necessary to carry out work to assess and mitigate risks of double-spending (through a combination of operational, regulatory and technological measures).
Token history vs performance	Token stores history of transactions. The more transactions are made with the token, the more data needs to be transferred upon each subsequent transaction.	At the next stages of the project, performance testing must be carried out and a solution must be developed to reissue a token to clear its history.
Confidentiality vs restorability of wallets	Token confidentiality is an important property of the payment system. At the same time, absolute confidentiality does not allow to restore the wallet if you lose access to it.	It is assumed that the chosen mechanics to manage user keys in the pilot project will allow restoring user wallets without affecting the confidentiality of transactions. A separate study of the procedure and technology for wallet restoration is required within the following stages.
Anonymity vs programmability	To verify the validity of tokens in a transaction, the remittee must be able to execute smart contracts for all transactions that have been performed in a given token's history. Therefore, smart contracts cannot operate on the amounts of transactions, balances, and personal data of participants and customers, since this data is blinded from the remittee.	It is necessary to find a balance between anonymity and programmability: some contracts may use special cryptographic methods (for example, non-interactive ZKP) to enforce restrictions without disclosing private data, however, in order to participate in other contracts, it may be necessary to sacrifice privacy by disclosing some of the token data. The target solution must be selected based on the results of a technological study of possibilities of creating smart contracts on the DT platform.

2.6 Comparison with CBDC projects in other countries

According to recent BIS statistics (October 2021), 26 central banks around the globe are piloting CBDC projects. Different central banks consider local specifics and market needs to choose approaches and options for CBDC implementation, combining new technologies tested on alternative currencies with traditional ones.

The most relevant examples are countries that have made significant progress in the creation of tokenized retail digital currencies, with already established interaction between the central bank and other participants of the financial market.

The experience of central banks which have made the greatest progress among other jurisdictions is the most relevant to Kazakhstan:

- **People's Bank of China** has advanced the most in CBDC implementation - in parallel with systematic scaling-up of e-CNY in the local market, PBOC is already implementing pilot projects with other countries on cross-border CBDC payments.
- **Bank of Sweden** was the first in Europe to start piloting CBDC, is now working on a regulatory approach to implementation, in parallel with a detailed step-by-step study of technological aspects jointly with banks and device vendors.
- **Bank of Russia** developed the concept and started the development of a technological platform, announcing piloting with 12 banks in 2022.

Key features of CBDC implementation in these countries in comparison with NBK are the following:

- ✓ In all of the above-mentioned countries as well as in Kazakhstan, a two-tier digital currency model is being piloted, where central banks develop the design and basic functionality of the platform, and second-tier banks and other financial organizations are responsible for connecting citizens and providing services to the population.
- ✓ Access type affects transaction flow within the platform, programming capabilities, and configuration of privacy of participants' transactions. Meanwhile, Sweden, similar to the NBK, implements a token-based accounting model, Banks of China and Russia base their currency design on a hybrid model: an intermediate model with both token-based model elements and a traditional account model.
- ✓ Storage of user tokens affects offline payments. Bank of Sweden, as part of piloting its e-krona, has opted for an approach with storing users' tokens on nodes of their banks. In Kazakhstan, storing tokens on the user's device model has been implemented, which makes it possible to make payments offline when the Internet is suddenly disconnected.

2.6 Comparison with CBDC projects in other countries

- ✓ All of the central banks have expressed interest in offline payments functionality. Currently, the offline payments functionality of the pilot platform has been implemented in Kazakhstan: users can make purchases when the Internet is unavailable to both the client and the seller. It is known from open sources that China and Sweden have begun testing the technological implementation of this type of transaction. Along with that, there is no information on the stage of development of this issue in other countries.
- ✓ China has implemented a 'controlled level of anonymity' approach with different levels of disclosure of information about the transaction, including dependence on the amount of transfer. Bank of Sweden also considers implementing different levels of anonymity for users' wallets. The NBK has tested the concept of customizable anonymity with the ability to control access to information about transactions and an option to customize data blinding on request of the user: Users can choose whether to show personal data to other participants in a transaction or not.
- ✓ Programmability was implemented within the pilot project in Kazakhstan, which allows putting restrictions on spending in the structure of the token itself (special purpose use). There is no public information about the possibility of customizing the special purpose of tokens in other countries.

As a result of the analysis of CBDC development projects in other countries, it can be concluded that most central banks have already joined the race, however, there is no mature and well-established practice yet - this is still an area for research and experimentation. Despite the common approach to the architecture of digital currencies, other parameters will vary depending on the goals and the solutions on key implementation forks.

Based on the results of the pilot project a list of open questions has been identified that should be studied in the future for possible implementation of the DT.

2.6 Comparison with CBDC projects in other countries

Comparison with CBDC projects in other countries

COUNTRY	YEAR	OBJECTIVES	CURRENT STATUS	KEY FEATURES
 CHINA	2014	<ul style="list-style-type: none"> Ensure financial availability and develop competitive advantages Improve efficiency of trans-border expenses 	<ul style="list-style-type: none"> Trial operation (test– 9 cities, 140 million users) Cross-border test scheduled for 2022 Olympiad 	<ul style="list-style-type: none"> Hybrid (account and tokens) One wallet in one bank (+ sub-wallets) Anonymous transactions (for a small amount) Offline (LCD – cards)
 SWEDEN	2017	<ul style="list-style-type: none"> To offer an alternative to cash as cash has mostly disappeared from circulation in Sweden Increase availability of money of the central bank 	<ul style="list-style-type: none"> 1st stage of the pilot project was implemented in 2020-2021 Regulation and engineering aspects are under elaboration 	<ul style="list-style-type: none"> Decentralized (based on tokens, DLT) Several wallets in several banks Controlled level of anonymity Long-term offline
 RUSSIA	2020	<ul style="list-style-type: none"> Improve speed, convenience and safety of payments Reduce level of cash use 	<ul style="list-style-type: none"> Implementation of platform prototype before the end of 2021 Pilot with 12 banks is scheduled for 2022 	<ul style="list-style-type: none"> Hybrid (online – account, offline – token) One wallet. Access from several banks No anonymity Offline (under elaboration)
 EU	2020	<ul style="list-style-type: none"> Support digitalization and strategic independence of the EU Enhance role of the Euro in international trade 	<ul style="list-style-type: none"> Decision is made to launch pilot 	<ul style="list-style-type: none"> Under elaboration
 USA		<ul style="list-style-type: none"> Support USD as an international reserve currency Reduce level of cash use 	<ul style="list-style-type: none"> Digital Dollar Foundation 5 pilot programs are scheduled until mid 2022 	<ul style="list-style-type: none"> Decentralized (tokens, DLT) Offline (under elaboration)



Economic and Regulatory Aspects

pages **73-90**

Due to the lack of international experience in addressing issues of full-fledged implementation of CBDC into the system of financial and economic relations, there are still open questions about economic consequences and risks that may result from CBDC issuance.

There are three key areas in which such risks may arise:

1. the impact of CBDC issuance on the volume of money supply, inflationary processes, and, consequently, the stability of the country's monetary policy, as well as transmission channels
2. the financial sector's response to the implementation of CBDC in the context of financial stability
3. the impact of CBDC on the current and prospective business conditions of the financial sector.

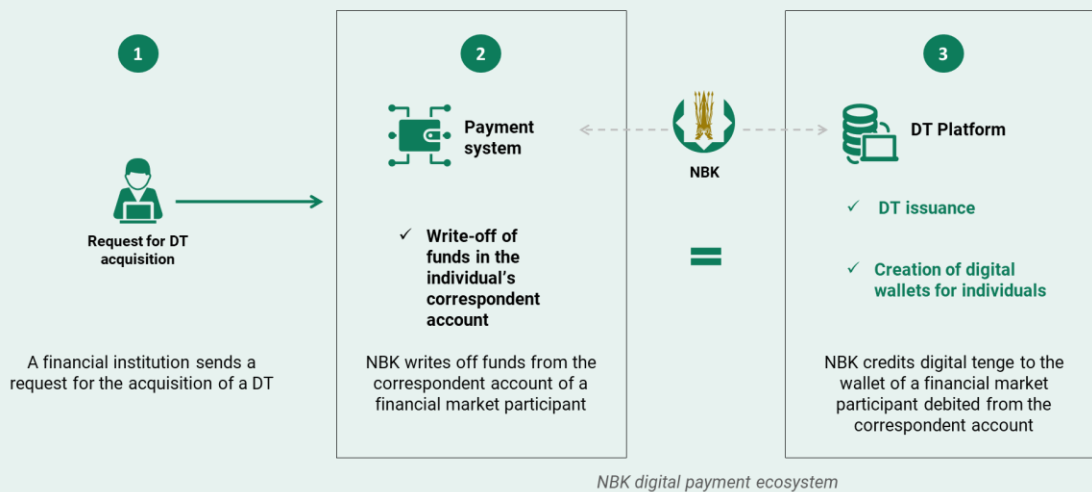
As part of a pilot project, a theoretical economic model of the DT was formulated and developed in order to test these risks in the current conditions of Kazakhstan's economy. It is important to note that this model is currently not a final and exhaustive methodological approach in the economic analysis of the DT. Consequently, in the future, as the empirical data will be collected and the theoretical parameters will be quantified, the model can be supplemented, modified, and expanded. At the same time, even at this stage, the model allows us to analyze several economic aspects of the issue and introduction of DT as a first approximation.

Theoretical DT economic model

The theoretical economic model of the DT is based on the technical design of digital currency issuance selected in the pilot project, where a two-tier digital payment system with three agents represented by the NBK, second-tier banks (STBs) and the end client is assumed.

Within this design, DT is issued at the request of STBs to the NBK. As a result, the NBK credits a requested DT amount to a digital wallet of the STB and debits a similar amount of funds from a correspondent account of the STB (see figure below). Further, the STB, in its turn, upon the client's request, credits a necessary DT amount which he needs to his digital wallet account, in return deducting a corresponding amount of cashless funds from his current account.

Technical design of DT issuance



Based on the technical design of DT issuance as presented above, its theoretical economic model assumes the presence of three economic agents:

- The NBK is the only and ultimate DT issuer
- Bank A is a second-tier bank that provides clients with financial services
- Alibek is an individual, a client of Bank A.

Within the theoretical model, the influence of the issuance and DT flow between agents is studied based on an analysis of their simplified balances. At the same time, the use of simplified balances of economic agents makes it possible to analyze DT dynamics in the context of conventional indicators of monetary statistics, in particular:

- RM – monetary base or reserve money, which includes direct liabilities of the NBK as cash outside the NBK, correspondent accounts of the Bank and its funds on a digital wallet account (so-called 'digital cash')
- M0 – monetary aggregate through which cash in circulation is recorded
- M0_dt – monetary aggregate reflecting a DT volume issued by the NBK ('digital cash')
- C - current (cashless) customer accounts in Bank A
- M1 - conditional money, representing a broad money supply as a sum of components M0, M0_dt and C.

3.1 Economic aspects

Within the theoretical model in the format of balances of economic agents, three stages of DT issuance were studied, taking into account its impact on indicators of monetary statistics:

- First stage: the situation in the economy before DT issuance
- Second stage: DT issuance in the form of its accrual by the NBK to the digital wallet account of Bank A
- The third stage (option 1): crediting the DT from the digital wallet account of Bank A to the digital wallet account of Alibek, a client of Bank A based on converting cashless funds from the current account
- The third stage (option 2): crediting the DT from the digital wallet account of Bank A to the digital wallet account of Alibek, a client of Bank A, based on the use of cash assets.

Next, we will cover the theoretical model DT issuance in stages, following the stages indicated above.

The first stage - DT is still missing in the economy

Balances of economic agents before DT issuance (KZT at current prices)

NBK			
Assets		Liabilities	
Not considered		Corr. account of Bank A	3000
		Cash outside of NBK Cash of Bank A	1000
		DT account (DT reserves)	0
Banks A			
Assets		Liabilities	
Corr. account of Bank A	3000	Alibek's current account	700
Cash of Bank A	1000	Other clients	3300
DT account of Bank A	0		
Alibek			
Assets		Liabilities	
Current account at Bank A (C)	700	Not considered	
Cash (M0)	550		
Alibek's Digital Wallet	0		

Within the first stage, which reflects an original situation in the economy, when the NBK did not issue the DT, the following amounts of funds in the economy are conditionally assumed:

- 3,000 KZT as a correspondent account of Bank A (part of the RM monetary base)
- 1,000 KZT – cash assets outside the NBK (part of the RM monetary base)
- 700 KZT – the volume of Alibek's current account (part of component C included in the broad money supply M1)
- 3,300 KZT – the volume of a current account of other clients of Bank A (outside the analytical consideration of the dynamics of the DT, it is a part of component C)
- 550 KZT - cash assets of Alibek (monetary aggregate M0).

Thus, it can be determined that in the context of monetary statistics, the original situation in the economy is as follows:

- $RM = 4000$ KZT
- $M0 = 550$ KZT
- $M0_{dt} = 0$ KZT
- $C = 4000$ KZT
- $M1 = 4550$ KZT

The second stage - the NBK, at the request of Bank A, issues

Balances of economic agents after issuance of the DT (KZT at current prices)

NBK			
Assets		Liabilities	
Not considered		Corr. account of Bank A	2000
		Cash outside of NBK Cash of Bank A	1000
		DT account (DT reserves)	1000
Bank A			
Assets		Liabilities	
Corr. account of Bank A	2000	Alibek's current account	700
Cash of Bank A	1000	Other clients	3300
DT account of Bank A	1000		
Alibek			
Assets		Liabilities	
Current account at Bank A (C)	700	Not considered	
Cash (M0)	550		
Alibek's Digital Wallet	0		

At the second stage, the NBK issues 1,000 KZT as DT at the request of Bank A. At the same time, in liabilities of the balance sheet of the NBK, therefore, in assets of the balance sheet of Bank A, 1,000 KZT are credited to the digital wallet account as a digital analog of cash assets. In turn, accrual of 1,000 DT units takes place due to the write-off of a similar amount of funds from a correspondent account of Bank A in the NBK, which is accordingly disclosed on the balance sheets of both economic agents.

As a result of this operation, it can be seen that the total volume of the NBK's liabilities (monetary base) does not change, as does the volume of Bank A's assets. At the same time, the structure of the monetary base and assets of Bank A changes.

Thus, at the second stage, key indicators of monetary statistics in the form of the monetary base RM and broad money supply M1 remain unchanged, amounting to 4,000 KZT and 4,550 tenge, respectively.

The third stage (option 1) - accrual of the DT to the account of Alibek's digital wallet based on the use of the current account

Balances of economic agents after DT is credited to the end customer's account based on the conversion of cashless funds (KZT in current prices)

NBK			
Assets		Liabilities	
Not considered		Corr. account of Bank A	2000
		Cash outside of NBK Cash of Bank A	1000
		DT account (DT reserves)	1000
Bank A			
Assets		Liabilities	
Corr. account of Bank A	2000	Alibek's current account	200
Cash of Bank A	1000	Other clients	3300
DT account of Bank A	500		
Alibek			
Assets		Liabilities	
Current account at Bank A (C)	200	Not considered	
Cash (M0)	550		
Alibek's Digital Wallet	500		

The third stage of the theoretical model describes a moment of direct accrual of the DT to Alibek's account in the amount of 500 KZT. At the same time, in the first option, this process is performed at the request of Alibek to Bank A, within a number of funds of 500 KZT is remitted to Alibek's DT account, and a similar amount is debited from the client's current account, which is in liabilities of Bank A. As a result, in liabilities of Bank A, the size of the current account belonging to Alibek is reduced by 500 KZT, and the amount of funds on the digital wallet account in the assets of Bank A, which at the second stage was accrued by the NBK, is reduced by the same amount. In other words, after 500 KZT in the digital form is credited to Alibek's account as a whole, the overall balance of Bank A decreases by this amount.

3.1 Economic aspects

In turn, in the assets of Alibek, there is a flow of funds from the current account to the DT account. As you can see, in this case, the DT, like cash, remains as the obligations of the NBK but not Bank A.

If we consider this stage of the DT issuance through the prism of monetary statistics indicators, the following will be seen:

- RM = 4000 KZT
- M0 = 550 KZT
- M0_dt = 500 KZT
- C = 3500 KZT
- M1 = 4550 KZT

The third stage (option 2) – DT is credited to the account of Alibek's digital wallet based on the use of cash assets

Balances of economic agents after DT is credited to the end customer's account based on converting cash assets (KZT in current prices)

NBK			
Assets		Liabilities	
Not considered		Corr. account of Bank A	2000
		Cash outside of NBK Cash of Bank A	1000
		DT account (DT reserves)	1000
Bank A			
Assets		Liabilities	
Corr. account of Bank A	2000	Alibek's current account	700
Cash of Bank A	500	Other clients	3300
DT account of Bank A	500		
Alibek			
Assets		Liabilities	
Current account at Bank A (C)	700	Not considered	
Cash (M0)	50		
Alibek's Digital Wallet	500		

3.1 Economic aspects

Another option of the third stage of the theoretical model of DT issuance assumes that the client of Bank A, Alibek, will use funds as cash to add DT to his account in the amount of 500 KZT. In this case, Alibek's cash is remitted to the corresponding account in the assets of Bank A, and the same amount of DT is transferred from the account of the digital wallet of Bank A to the account of Alibek's digital wallet. As a result, there will be no change in the size of the balance sheets for both Bank A and the client. In monetary statistics, this process will be reported as follows:

- $RM = 4000$ KZT
- $M0 = 50$ KZT
- $M0_{dt} = 500$ KZT
- $C = 4000$ KZT
- $M1 = 4550$ KZT

Next, let us compare changes in indicators of monetary statistics in situations before the issuance of the DT and after it was received on the account of the end client of Bank A both through the use of cash and through the use of funds on a cashless (current) account.

Provisional figures of monetary statistics before and after DT issuance (tenge in current prices)

Parameters of monetary statistics	Before DT issuance	After DT issuance: option when DT is converted at the expense of cashless funds of a client	After DT issuance: option when DT is converted at the expense of cash funds of a client
Monetary base, RM	4000	4000	4000
Cash in circulation, M0	550	550	50
Digital cash in circulation, M0 _{dt}	0	500	500
Current (cashless) funds, C	4000	3500	4000
Monetary offer, M1	4550	4550	4550

As it can be seen from the table above, the issuance of the DT in none of the two options causes an increase in the monetary base (liabilities of the NBK) or an expansion of the money supply.

At the same time, when the DT is issued and credited to the client's account based on the conversion of the current account, there is only a change in the structure of the money supply, namely, a decrease in volume of current accounts due to an increase in the volume of DT. In case when the conversion of the DT takes place as a result of the use of cash, then in structure of the money supply size of current accounts does not change but cash assets in circulation shrink.

Thus, the main result obtained in the analysis of the theoretical economic model of DT is the following. The issue of the digital analog of cash will not increase the monetary base and money supply in the economy of Kazakhstan, and only changes in the structure of the money supply will be observed.

The following economic conclusions can be derived from the economic model:

1. The issue of the DT does not affect the expansion of the money supply, so no direct impact on the aggregate demand of the economic agents. Consequently, inflationary processes remain outside the direct or exclusive effect of the DT issuance.
2. The issuance of the DT does not pose significant or uncontrollable risks to the financial market both in case of conversion of cash of end clients and in case clients of STBs prefer to convert part of their current (non-cash) accounts into DT. Thus, currently, the banking sector of Kazakhstan has an excessive level of reserves, which will be able to fully cover possible options of current accounts reductions.
3. In case of necessity related to possible excessive outflow of funds on current accounts of STBs to customers' CT accounts NBK will potentially be able to fully provide the required amount of liquidity for STBs within the framework of using instruments of the monetary policy. This factor will level the risks of 'digital run' when in times of crisis the banks' clients may be motivated by the maximum conversion of non-cash funds into digital currency. This factor also reduces the risks of significant deviation of rates in the money market from the current levels of the prime rate.
4. Risks of 'digital run' may be limited by mechanisms that limit acceptable volumes of conversion from current accounts into DT and other measures of financial regulation.
5. The above-stated conclusions indicate that the process of issuance and use of the DT as the third form of fiat money in Kazakhstan (along with cash and cashless funds) is not a source of risks both the stability of monetary policy and channels of its transmission mechanism as well as and for the stability of the financial system.

5. In terms of the impact of the use of the DT on current and future business conditions of the financial sector, the following should be noted:
- the use of DT potentially enables a larger coverage of potential clients with financial services, who previously remained 'in the shadow of cash' due to geographical, technical, cultural, and behavioral restrictions and peculiarities, including as part of further integration of clients into their ecosystems of financial institutions
 - the introduction of DT creates infrastructure conditions for the development of completely new fintech products based on advantages of digital cash, faster and cheaper fintech services (for example, Embedded Finance, M2M payments, IOT-enabled payments, etc.)
 - with the current platform (ecosystem) business model of financial institutions, use of the DT by end customers will reduce the dependence of several financial institutions on the 'transactional model of earnings' encouraging them to work in conditions of 'economies of scale' and increase their 'network effects' directions of financial activities.

Further steps of economic aspects of the DT

In the future, a study of behavioral aspects of financial services consumers in Kazakhstan will be carried out about their payment patterns: use of existing means of payment in the form of cash and cashless money within the trade and economic transactions in the domestic market as well as in terms of the potential use of DT for same purposes. It is assumed that this study will be implemented, including surveys with focus groups, to collect and accumulate a critical set of empirical data.

Along with that, it is planned to conduct a full-fledged scientific and practical study for an in-depth study of macroeconomic effects of DT, that will be based on data obtained through surveys of consumers of financial services. It is expected that the findings of this study will provide a quantitative assessment of the parameters presented in the theoretical DT economic model, which was formulated during the pilot project phase (see 2.4).

Important economic aspects, which will also receive special attention, are issues related to cross-border payments and import operations based on DT use.

The creation of a comprehensive regulatory environment with a high level of legal certainty is one of the key issues to be worked out within the pilot project for the implementation of a national digital currency.

Questions as to whether the central bank is authorized to issue CBDC or whether CBDC can be a legal means of payment affect the fundamental relationship between money, government, and law. These issues have practical importance since the CBDC must have a solid legal basis for widespread public use. In the absence of a sound legal basis, CBDC issuance poses legal, financial, and reputational risks for central banks. While a proper design of the legal framework will depend to some extent on the design specifics of the CBDC, there are nevertheless some implications in this area of study.

In the context of these issues, the IMF researchers have analyzed regulations of 174 central banks with an emphasis on two of the most important public law aspects of the CBDC – legal framework of the CBDC in subject to the laws on the central bank and its regime in line with the monetary laws [\[30\]](#).

Legal aspects of various CBDC designs

Design of CBDC access technology based on accounts and tokens

The legal status of accounts under private and public law is well developed and understood. Digital tokens, on the other hand, do not have a long history, and their legal status under public and private law currently requires further elaboration.

First, token-based CBDC is a claim to the central bank. By analogy with the transfer of banknotes and coins, the transfer of a token is equivalent to the transfer of a claim. This is what distinguishes token-based banknotes, coins, and CBDC from money in accounts and bills of exchange (debt securities), which are transferred to debit and credit between current cash accounts and securities accounts, respectively.

Second, for both tangible and digital forms of tokens, the holder must either own banknotes/coins or know a password that allows him to manage the currency. If an owner loses either banknotes/coins or his password, he will no longer be able to use the currency. Whereas account owner, if the password is lost, will still be able to use the funds as long as he can confirm his identity to the organization that confirms his account.

Third, in the taxonomy of central bank liabilities, a token-based CBDC is neither money in accounts nor a bill of exchange. In case that CBDC is issued to the general public, it will have a common feature with banknotes and coins that are also issued for wide distribution.

<p>Availability to consumers</p> <p>Wholesale and retail CBDC</p>	<p>Some central banks study an opportunity to issue CBCD only to existing account holders and participants in RTGS payment systems. These are mainly (large 'clearing') banks and public authorities ('wholesale'). Other central banks use the network much more extensively and tend to offer CBCD to the general public ('retail') rather than to offer it to wholesale customers. Finally, some central banks believe that their CBCD must be 'general purpose' and accessible to both wholesale and retail counterparties.</p> <p>From a legal point of view, this distinction is appropriate in cases where CBCD is designed as an account. Laws of a lot of central banks restrict categories of legal entities and individuals that can open such accounts. Other important legal issues are anti-money laundering regulations and competition law.</p>
<p>Access to implementation of the architecture</p> <p>Direct, indirect and hybrid</p>	<p>Certain central banks study an opportunity to issue CBDCs in a direct or single-tier form: they will issue CBDCs and independently manage their circulation. Other financial institutions study an issuance as an indirect 2-tier form (also called 'synthetic'), whereby liabilities are issued by a commercial bank but are completely backed by the central bank. The hybrid form will consist of direct claims to the central bank and payment intermediaries.</p> <p>From a legal point of view, two important questions arise. First, to qualify as a CBDC, 'currency' must become a direct responsibility of the central bank; that's what makes it risk-free. Obligations of commercial banks, even if they are backed by a 100% cash deposit in books of the central bank, are not those of the latter. Second, in the case of a token-based digital central bank, the question arises as to whether and under what conditions the legal framework allows 'entry' of the central bank into ledgers of commercial banks.</p>
<p>Approach to arrangement of technological infrastructure</p> <p>Centralized and decentralized</p>	<p>Central banks are debating whether CBDC transfers will be centralized - as in the currently existing RTGS - or decentralized with the use of distributed ledger technology (DLT). As for the latter, an additional variable will be whether the DLT will operate on an open or closed basis. Given the impact that DLT can have on an open basis, including potentially complicating the central bank's ability to manage the money supply, it is most likely that central banks will choose closed-type DLT. Discussions are still underway with respect to the legal implications of this choice.</p>

While design features have some legal implications, the distinction between account-based and token-based CBDC has the most significant legal implications. In this regard, many open questions need to be worked out in the context of token-based DTs. In order to adequately assess legal differences between checking accounts and DTs based on tokens processed centrally or through a closed DLT, it is necessary to emphasize the legal distinction between current cash accounts and (general) ledger accounts.

Cash current accounts are a banking method and represent a special contractual and legal relationship between a financial institution and an account holder. Consequently, the rights and obligations of the parties are primarily provided for by the contractual terms and conditions regulating the account. Statutory provisions and general legal principles may also apply. In most jurisdictions, cash current accounts operate based on a mutual agreement of the Roman law: although funds credited to the account are called 'deposits', the financial institution does not have to keep these funds but only has the right to use them in the future. Credit balances on cash current accounts are transferred under debit and credit between accounts.

Ledger accounts are an accounting method and not a contractual concept: they represent a financial standing of a reporting entity based on subaccounts established by a chart of accounts of the entity. General ledger accounts can represent an asset, liability, income, or expense. General ledger accounts by themselves do not establish or represent a legal relationship between a reporting entity and a third party and do not create rights and obligations between a reporting entity and other parties (However, nothing prevents a reporting entity and third parties from entering into a contractual relationship.)

The ultimate legal implication of this difference is that, while a token-based CBDC can be represented by a central bank in centrally managed ledger accounts, it is not a credit balance in a checking account. This means that there is no contractual relationship between the central bank and a holder of a token-based CBDC, except for an (admittedly very specific) requirement included in the token, very similar to the legal status of banknotes. Nevertheless, IMF experts have developed several recommendations for central banks considering digital currencies based on tokens that are applicable in Kazakhstan.

Need to reform laws related to the Central Bank

The absence of a clear and reliable legal basis for CBDC issuance based on tokens and/ or accounts entails a targeted reform of the laws related to the central bank.

According to recommendations for CBDC issuance on the basis of tokens, it is logical to introduce the following amendments to the laws related to the Central Bank:

1. Central bank law must describe a clear function of currency issue' in general, without restricting issue solely in the form of banknotes and coins.
2. Relevant powers to exercise this function must be formulated, where appropriate, with a clear reference to the issue of currency in the form of banknotes (and possibly coins) as well as in the form of a digital token.

A key argument in favor of introducing a clear legal framework is that, depending on an intended design, this amendment will support more innovative features of the CBDC (for example limited privacy and general availability).

To provide a legal basis for CBDC issuing on the account basis, in particular, the laws on the central bank should be amended to expand the specific powers to open current accounts. For example, by mentioning the general public in the central bank law or by the competent authority making decisions on the categories of individuals and entities that will have access to the current accounts in the central bank's books.

Concerning both types of CBDC, careful consideration of the payment system functions with its limitations by interbank payment systems is required.

It is necessary to make appropriate changes in the legislative acts regulating and defining the basis for the issue of money, money circulation, and monetary relations

Some of the questions raise fundamental and conceptual legal policy issues that require careful analysis and strategy definition by competent political authorities. Moreover, the possible participation of the state in reforms of monetary legislation to ensure CBDC issuance may be limited by the provisions of the Constitution of the Republic of Kazakhstan.

To legally equate token-based CBDC with banknotes, significant monetary reform will be required. According to IMF research, countries are encouraged to first consider whether or not this type of CBDC must get a status of legal means of payment. One option in this regard is to restrict this status to a closed category of certain legal entities (government, public authorities, and traders outside a certain size and/ or firms with permitted activities such as banks).

3.2 Regulatory aspects

As a next step, countries are encouraged to analyze the private legal classification of CBDC based on tokens and question of whether this new form of money must be privileged subject to the private law (in particular, to facilitate its circulation). As a third step, authorities are encouraged to revise definitions of cybercrime offenses to clearly cover cybercrime offenses against CBDC.

Talking about account-based CBDC – at this stage, it is not needed to carry out monetary reform for account-based CBDC.

It is necessary to point out that possible introduction of the DT will affect regulatory aspects related to the Law 'NBK of the Republic of Kazakhstan', tax laws, private law (including property law), contract law, laws related to payments and payment systems, laws related to rehabilitation and bankruptcy, laws related to personal data and their protection, international private law. Moreover, effective implementation of the AML/CFT system needs to be carefully considered. This list may not be exhaustive and will be amended based on findings of further research.

Open questions for further elaboration

Description	Aspects for further elaboration
DT definition	<p>Determination of DT status and role as a new form of money, including a change in the existing regulatory legal acts in terms of regulating interest rates within the conduct of the monetary policy.</p> <p>Establishment of the DT as an official monetary unit, mandatory to perform a function of a means of payment.</p> <p>Determination of the DT as a separate type of cashless funds.</p>
Roles of participants and NBK	<p>Determination of participant roles regulation: rights and obligations of participants of the digital platform.</p> <p>Determination of responsibilities of the NBK as a digital platform operator: rights of the NBK to carry out banking operations using DT with credit institutions, legal entities, and individuals.</p> <p>Distribution of responsibility for the operation of the information system, within which CBDC circulation takes place.</p>
Requirements to participants	<p>Determination of criteria and requirements for financial players, including the elaboration of liquidity requirements, operational rules for distribution, and limits on the use of the DT to limit capital flows from commercial banks.</p> <p>Elaboration of requirements for KYC checks at participants of the financial market, the definition of criteria and requirements for AML inspections, considering confidentiality and a possibility of anonymous payments.</p>
Security	<p>Elaboration of requirements and criteria for protection of personal data of users that constitute bank secrecy, and distribution of responsibility between the participants.</p>
DT use	<p>Elaboration of the legal regime for use of the DT in civil law relations, including amendments to provisions of the laws that regulate a field of settlements and establishing specifics for discharge of monetary obligations using the DT.</p> <p>Elaboration of changes in the field of tax and budgetary laws, modifications in regimes of foreclosure on the property (including determination of specifics of managing a digital wallet within relations related to bankruptcy).</p>
Technical requirements	<p>Elaboration of technical standards and requirements for DT functioning, including interoperability, programmability, security, scalability.</p> <p>Choose a model of access to the CBDC depending on legal relationship and elaboration of appropriate regulation (direct access, hybrid through a payment / technical service provider, indirect through intermediaries).</p>

3.3 Wholesale transactions

In addition to exploring the possibilities of DT in retail payments, NBK also plans to consider the potential for using DT in wholesale transactions and payments between organizations.

The use of the DT platform can significantly increase the efficiency of mutual settlements between market players, which is achieved by ensuring trust in the distributed ledger system. The ability to make the transfer directly without intermediaries can significantly simplify mutual settlements between market participants, for example, in supply chains or for immediate final settlements in the securities market.

In addition to improving efficiency and reducing costs in existing interbank settlements, DT can also enable the implementation of new effective instruments for market participants: in particular, the tokenization of various types of assets allows the use of CBDC for immediate low-risk settlements in DvP (delivery versus payment).

3.4 Cross-border payments

The possibilities of DH in cross-border payments will be further explored in partnership with international organizations and other central banks

Potential for the development of cross-border payments with the help of CBDC



Source: CPMI, BIS Innovation Hub, IMF, World Bank



Further steps

pages **92-95**

The pilot project in 2021 on the DT implementation enabled to lay off the foundation for the basic architecture of the national digital currency in Kazakhstan along with the definition of the key design parameters, technological approaches, as well as preliminary models to assess the economic aspects and the relevant regulatory framework. NBK emphasizes the high contribution of market participants' involvement and expert community for the progress of the study.

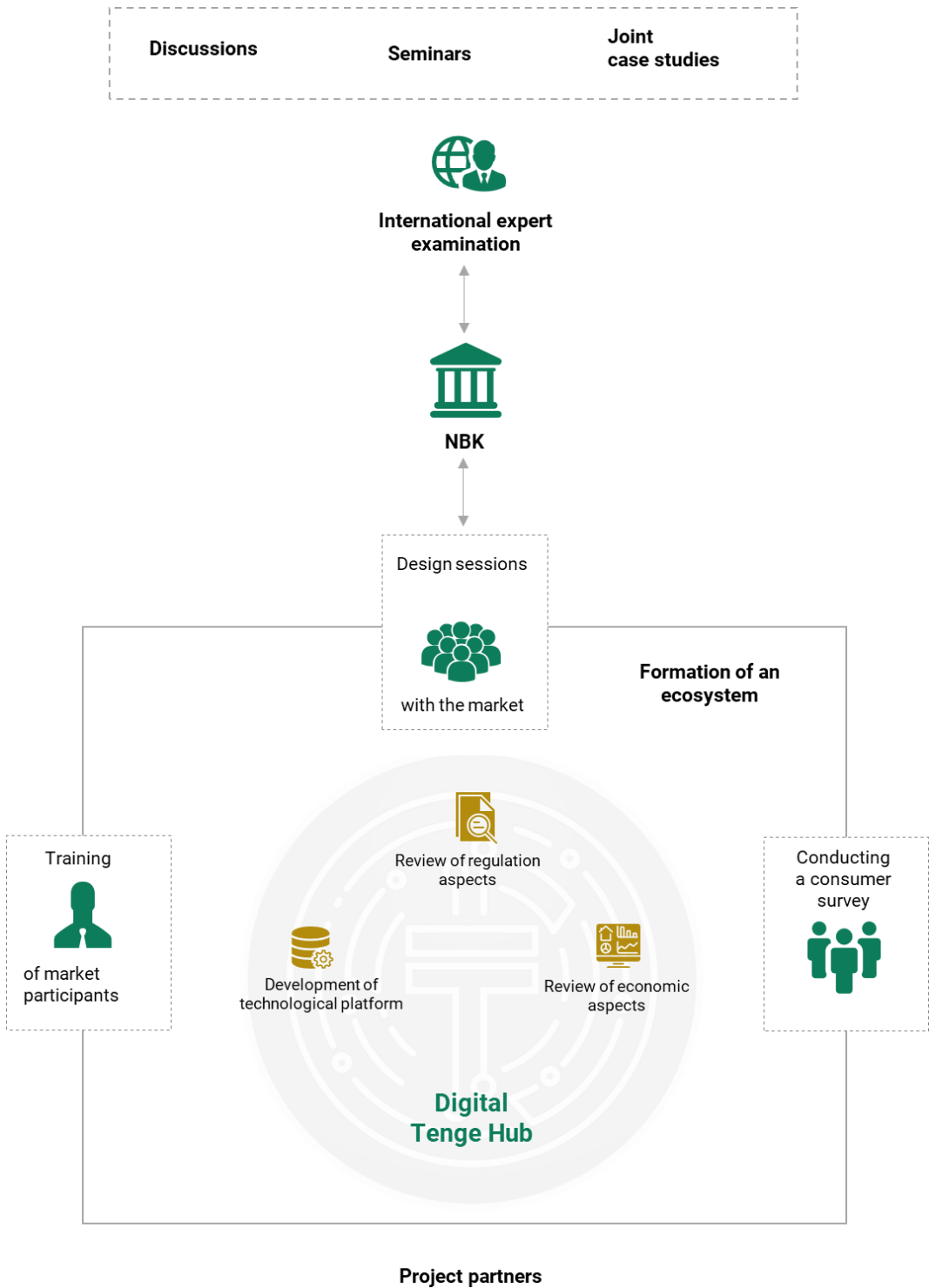
Based on the joint assessment of research results of this year with international partners (IMF, BIS, collaborative research institutes) as well as the analysis of similar works by other central banks, NBK has identified the following strategic milestones for further research:

- 1. Creation of the Digital Tenge Hub** collaborative platform to hold design sessions with market participants and the expert community. Also, it will enable the creation of a comprehensive collection of training resources and tools for them and allow them to work with the pilot platform based on the principle of a 'single window'. The NBK will pay special attention to the development of the DT ecosystem, including the assistance of market participants in the development of DT-based services. Digital Tenge Hub will be an important platform for the involvement of the market and experts in the decision-making process for the potential DT rollout.
- 2. Conducting a comprehensive economic study**, using the qualitative and quantitative methods, including the analysis of consumer patterns of payment instruments usage, qualitative and quantitative demand for perspective the DT, and the impact of a possible implementation on key economic parameters. Together with market participants, the effects on financial stability and business models of participants will be studied in detail, moreover, the measures to monitor related risks will be developed. Economic aspects of the design of the DT will be developed, including an accounting model.
- 3. Expansion of the pilot DT platform** functionality concurrently with the development of several technological issues, including aspects of scalability/performance, information security, interoperability with the existing payment infrastructure, etc. In a limited infrastructure, together with market participants and infrastructure players (including international payment systems), the functionality of key scenarios for using the DT platform will be tested.
- 4. Elaboration of regulatory aspects** of the DT introduction will make it possible to develop a list of specific recommendations for legal unambiguity and the creation of a balanced environment for the functioning of the DT. Necessary changes will be identified to consolidate vocabulary; roles, rights, and obligations of participants in DT turnover; regulatory mechanisms to control potential risks; AML/CFT aspects, etc.

The NBK of the Republic of Kazakhstan will ensure the development of a final model to decide on the introduction of the DT and perform a presentation of interim results of the study and discussion with all stakeholders in July 2022.

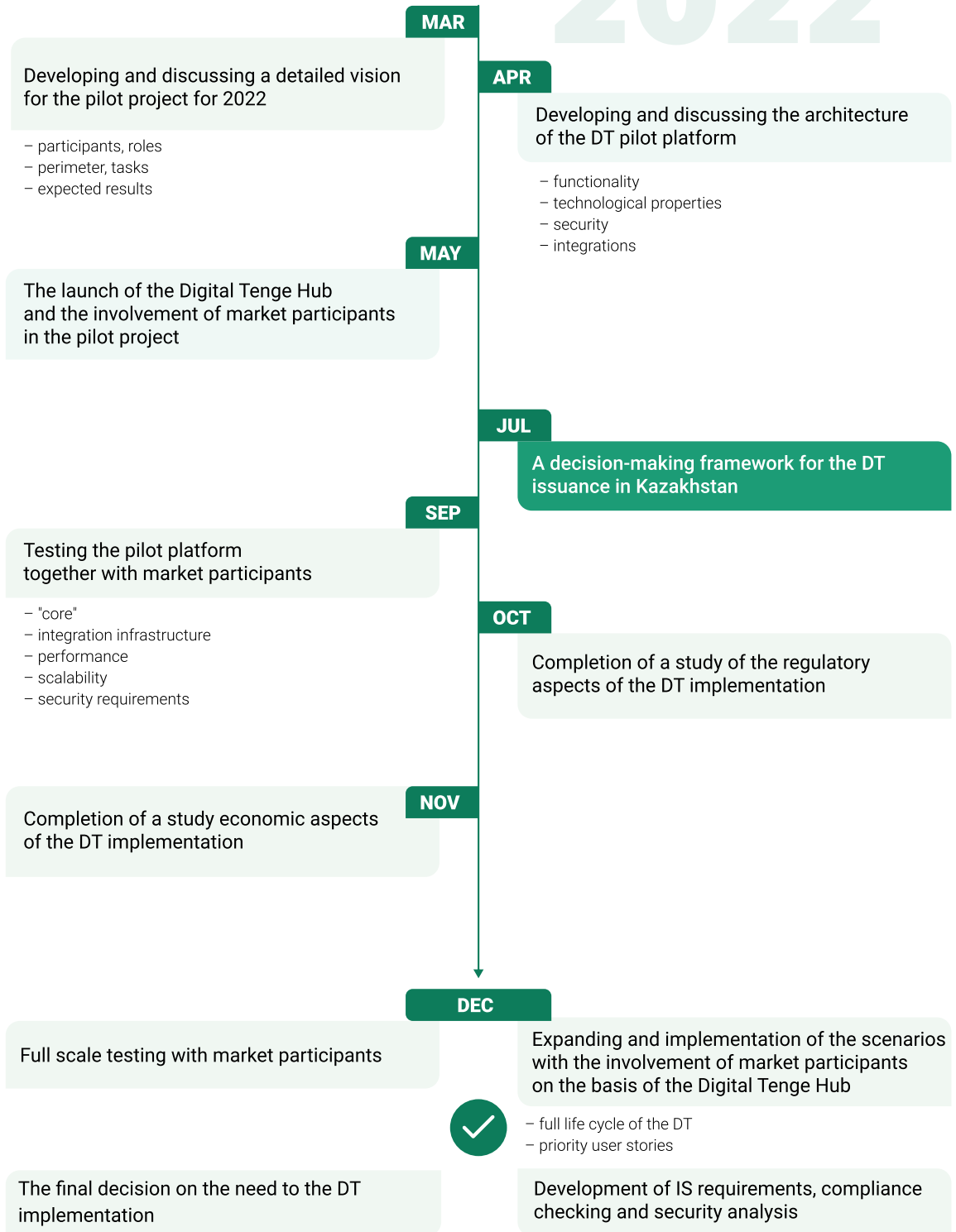
A decision on the need for the DT introduction will be made in December 2022, taking into account the final results of a comprehensive study based on the developed model.

Approach to studying DT in 2022



Areas of work, tasks, activities in 2022

JANUARY 2022



The National Bank will ensure active involvement and regular discussions of interim of the project results with all stakeholders during 2022

Expert feedback



Professor Jamiel Sheikh

**Founder The Central Bank Digital
Currency Think Tank**

**Author, Mastering Corda & The
Decentralized Finance
Phenomenon**

The Digital Tenge project, much like the word *tenge* means, represents a balance in the financial world. With the advent of cryptocurrencies and stablecoins, the global demand for new ways of representing, storing and exchanging value have been pushed to the forefront of the innovation frontier. Central banks around the world are responding, some with a wait, yet study it, approach and others with experimentation with some even deploying a solution and going live. The DT project by the National Bank of Kazakhstan is an exciting step in this direction of development. I am especially excited about the experimentation done to produce a DT that has offline capabilities, programmability and adjustable anonymity. These three represent some of the hardest problems and pose some of the hardest questions in the CBDCs. CBDCs can be easily dismissed as a surveillance coin and the NBK has risen to the occasion to show that this not need be the case.

The programmability of the DT, for example in the case of disbursement of cash, is a use case I have been studying for the past several years (I trademarked the word *Disburse* for payments in the US!) and shows that the NBK is thinking about a broad range of use cases. Although the paper produces some answers, some questions still linger and I eagerly wait to see now the NBK answers these questions in the future, including how a light client would work, what throughput, scalability and availability SLAs are needed. The paper does an excellent job explaining a number of interesting implementations in the experiment, including how a spend key is used, a treatise on a number scenarios and a detailed analysis of the DT's impact on indicators of monetary statistics. This is coupled with a deep analysis of regulatory aspects and implication.

The paper should be a shining beacon and light for other central banks, NGOs, academics, digital currency, cryptocurrency enthusiasts and anyone else that is looking to absorb some fresh and deep perspective on how a CBDC potentially can be implemented by a team like the NBK that is nothing less than genius.

Expert feedback



Willy Lim

Global Advisory Lead – Digital Currencies and Capital Markets, R3

The Digital Tenge project provided the National Bank of Kazakhstan an opportunity to investigate the feasibility and application of a general purpose CBDC in Kazakhstan. With the global economy rapid acceleration towards digital economy, there hasn't been the right time to prioritize the need for a payment instrument issued by trusted entity, promotes universal access and drives innovation. This is precisely the vision of Digital Tenge as Kazakhstan continue to grow the digital economy both domestic and internationally, securing itself as the growth and innovation center of Central Asia.

DT has allowed NBK to analyse innovative features such as programmable money, offline payments and the ecosystem that Digital Tenge can enable. Such features allow efficient implementation of important use cases that address digital literacy, delivery of efficient social payments and real time analytics which feed into accurate planning of key macroeconomic indicators. The feature of providing real time analytics is particularly exciting as it allows policy makers to accurately plan and implement various policy tools based on live accurate macroeconomic indicators to targeted sectors.

I commend the NBK on the delivery of this excellent report. The paper highlights answers on critical questions such as regulatory implications, application of DLT as mitigation for risk of central points of failure and application of programmability. Programmability is particularly exciting as it has the potential of improving efficiency and close gaps in fraud detection; and enabler of innovative services sought by users.

The successful completion of Phase 1, which culminates in this report, lays the framework for the Phase, allowing NBK to implement targeted use cases that address the needs of Kazakhstan. I congratulate the entire NBK team for this pioneering achievement.

List of references

1. Mngomezulu, Z., Rimer, S., Ouahada, K., Ndjongue, A. (2017). A review of Bluetooth and NFC for financial applications. In Sixth International Conference on Advances in Computing, Control and Networking-ACCN 2017 (pp. 48-51). <https://ujcontent.uj.ac.za/vital/access/services/Download/uj:24322/SOURCE1>
2. Igboanusi, I. S., Dirgantoro, K. P., Lee, J. M., & Kim, D. S. (2021). Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture. *ICT Express* <https://www.sciencedirect.com/science/article/pii/S2405959521000928>
3. Omilabu, A. A., Olusanya, O. O., Adebare, A. A., Ibitowa, F., & Longe, O. B. (2017). Comparative Analysis of Wi-Fi, Bluetooth & Xender Wireless Technology Applications. *Computing*, 8(4). https://www.researchgate.net/publication/349477834_Done_3_CISDI
4. Noether, S., & Mackenzie, A. (2016). Ring confidential transactions. *Ledger*, 1, 1-18. <http://ledger.pitt.edu/ojs/ledger/article/view/34>
5. Metere, R., & Dong, C. (2017, August). Automated cryptographic analysis of the pedersen commitment scheme. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 275-287). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-65127-9_22
6. Opare, E. A., & Kim, K. (2020). A compendium of practices for central bank digital currencies for Multinational financial infrastructures. *IEEE Access*, 8, 110810-110847 <https://ieeexplore.ieee.org/abstract/document/9115606>
7. Klein, M., Gross, J., & Sandner, P. (2020). The Digital Euro and the Role of DLT for Central Bank Digital Currencies. FSBC Working Paper, Frankfurt School Blockchain Centre https://researchgate.net/publication/341354711_The_Digital_Euro_and_the_Role_of_DLT_for_Central_Bank_Digital_Currencies
8. Scorer, S. (2017). Central Bank Digital Currency: DLT, or not DLT? That is the question. <https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/>
9. R3 Sandbox for Digital Currencies. <https://www.r3.com/digital-currency-sandbox/>
10. Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., ... & Zhang, F. (2020). Design choices for central bank digital currency: Policy and technical considerations (No. w27634). National Bureau of Economic Research <https://nber.org/papers/w27634>
11. DTCC, What we learned from our DLT capability study. A Q&A with DTCC's Jennifer Peve. <https://www.dtcc.com/dtcc-connection/articles/2018/november/08/what-we-learned-from-our-dlt-capability-study>
12. Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *Ict Express*, 7(2), 229-233. <https://www.sciencedirect.com/science/article/pii/S2405959520301909>
13. Han, R., Shapiro, G., Gramoli, V., & Xu, X. (2020). On the performance of distributed ledgers for internet of things. *Internet of Things*, 10, 100087. <https://www.sciencedirect.com/science/article/abs/pii/S2542660518300416>
14. Monetary Authority of Singapore and Accenture, Project Ubin (2016 – 2021) <https://www.mas.gov.sg/schemes-and-initiatives/project-ubin>
15. Accenture, The (R)evolution of Money: Blockchain Empowered Digital Currencies (2017) https://www.accenture.com/t20171116T025715Z_w_us-en_acnmedia/PDF-63/Accenture-Evolution-Money-Blockchain-Digital-Currencies.pdf
16. Accenture, The (R)evolution of Money II: Blockchain Empowered CBDC (2020) <https://www.accenture.com/us-en/insights/blockchain/evolution-money>
17. Accenture, Connecting ecosystems: Blockchain integration (2018) <https://accenture.com/us-en/insights/blockchain/integration-ecosystems>

List of references

18. Accenture and DTCC, Governing DLT Networks, DLT Governance for Private Permissioned Networks (2019) https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/global/2/accenture-governing-dlt-networks.pdf
19. ECB and Accenture, Exploring anonymity in central bank digital currencies with European Central Bank (2019) <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf>
20. Digital Dollar Foundation and Accenture, The Digital Dollar Project (2020) http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf
21. Riksbank and Accenture, The Riksbank's e-krona pilot (2018 – 2021) <https://www.riksbank.se/globalassets/media/rappporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf>
22. Corda. An analysis of Ethereum's recent chain split. <https://www.corda.net/blog/an-analysis-of-ethereums-recent-chain-split/>
23. Bickers K. Blockstream Sponsors Federated E-Cash as a Bitcoin Scaling Technology. <https://medium.com/blockstream/blockstream-sponsors-federated-e-cash-as-a-bitcoin-scaling-technology-637ba05de7b3>
24. World Economic Forum: Digital Currency. Governance Consortium. White Paper Series. Compendium Report, Nov 2021 https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf
25. Global CBDC Challenge Problem Statements organized by Monetary Authority of Singapore, November 2021 https://tribex.co/wp-content/uploads/2021/06/Global_CBDC_Challenge_Problem_Statements.pdf
26. Auer R., Cornelli G., Frost J. Rise of the central bank digital currencies: drivers, approaches and technologies. <https://www.bis.org/publ/work880.htm>
27. BIS: Central bank digital currencies: foundational principles and core features. Report # 1 in a series of collaborations from a group of central banks. https://www.bis.org/publ/othp33_summary.pdf
28. G7 United Kingdom 2021: Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf
29. BIS Annual Economic Report 2021 <https://www.bis.org/publ/arpdf/ar2021e3.pdf>
30. Bossu W., Itatani M., Margulis C., Rossi A., Weenink A., Yoshinaga A. Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>
31. DT. The Digital Tenge Public Discussion Report (May 2021) <https://nationalbank.kz/ru/page/cifrovoy-tenge-pilotnyy-proekt>
32. Registry of payment systems (2020) <https://www.nationalbank.kz/ru/news/reestr-platezhnyh-sistem>
33. Interbank clearing system <https://www.nationalbank.kz/ru/news/sistema-mezhbankovskogo-kliringa>
34. SMEP and SIP. <https://www.kisc.kz/catalog/smep>
35. Statistics of payments passing through the SMEP. <https://www.kisc.kz/catalog/177>
36. Payment cards and electronic banking services [11/2021] <https://www.nationalbank.kz/ru/news/elektronnye-bankovskie-uslugi?page=1>