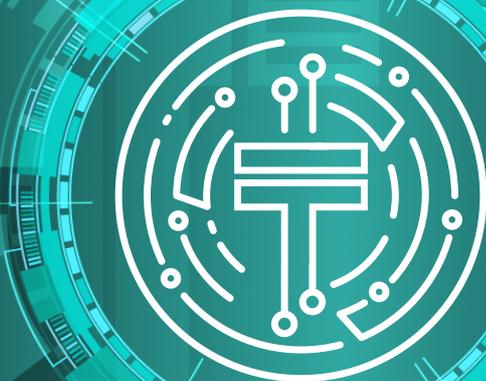




НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА



**РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ
О НЕОБХОДИМОСТИ ВНЕДРЕНИЯ
ЦИФРОВОГО ТЕНГЕ
WHITE PAPER 2022**

Содержание

Резюме	5
Введение	10
Цели, задачи и принципы внедрения ЦТ	14
<hr/>	
Технология	16
Дизайн ЦТ	17
Гипотезы и вопросы исследования	32
Подход к оценке	33
Результаты исследования	36
Выводы оценки	49
<hr/>	
Экономика	50
Дизайн ЦТ	51
Гипотезы и вопросы исследования	51
Подход к оценке	52
Результаты исследования	54
Выводы оценки	58
<hr/>	
Экосистема	59
Дизайн ЦТ	60
Гипотезы и вопросы исследования	61
Подход к оценке	62
Результаты исследования	62
Выводы оценки	70
<hr/>	
Операционная модель	71
Дизайн ЦТ	72
Гипотезы и вопросы исследования	72
Подход к оценке	72
Результаты исследования	73
Выводы оценки	82
<hr/>	
Регулирование	83
Дизайн ЦТ	84
Гипотезы и вопросы исследования	84
Подход к оценке	85
Результаты исследования	85
Выводы оценки	89
<hr/>	
Итоговая оценка	90
Дорожная карта	90
Список литературы	96
Приложения	101

Сокращения

API	(Application programming interface) Программный интерфейс приложения – описание способов, которыми одна компьютерная программа может взаимодействовать с другой программой
C2C	(Customer-to-customer) Платежи и переводы денежных средств между физическими лицами
DeFi	(Decentralized finance) Новые финансовые технологии, основанные на безопасных распределенных реестрах
DLT	(Distributed ledger technology) Технологии распределенных реестров – подход к обмену и хранению информации на нефиксированном числе узлов связи с использованием заданных алгоритмов достижения консенсуса для синхронизации копий данных между участниками
DSGE	(Dynamic stochastic general equilibrium) Динамическое стохастическое моделирование общего равновесия - макроэкономический метод моделирования поведения экономических на микроуровне.и стохастических шоков
ISO	(International organization for standardization) Международная организация по стандартизации
KYC	(Know your customer или Know your client) Знай своего клиента – процедура идентификации личности клиента
KPI	(Key performance indicator) Ключевой показатель эффективности
MVP	(Minimum viable product, минимально жизнеспособный продукт) Базовый, обладающий минимально необходимыми характеристиками продукт, позволяющий экспериментально проверить предположения и получить обратную связь от потребителей с целью формирования гипотез для дальнейшего развития
NFC	(Near-field communication) Технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами
PoC	(Proof of concept) Проект по разработке прототипа платформы (пилотной платформы) для проверки жизнеспособности концепции цифрового тенге
PoS	(Point of sale) Электронное программно-техническое устройство для приёма к оплате платёжных карт
Q&A	(Questions and answers) Вопросы и ответ
QR-код	(Quick response code) Код быстрого отклика
RTGS	(Real-time gross settlement) Система осуществления непрерывных расчетов по переводам средств в режиме реального времени
R&D	(Research and development) Экспериментальное исследование новых возможностей и сервисов использования цифровых валют
REST API	(Representational state transfer-based application programming interface) Архитектурный подход для создания программных интерфейсов приложения, основанный на передаче состояния представления
SHA-512	(Secure hash algorithm 512) Криптографический алгоритм, основанный на однонаправленных хеш-функциях
SSH	(Secure shell) Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой
TPS	(Transactions per second) Число транзакций, выполняемых в секунду
TLS	(Transport layer security) Криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет
UTXO	(Unspent transaction output) Вывод неизрасходованных транзакций, остатки криптовалюты, получаемые пользователем с каждой транзакции в блокчейне
UI/UX	(User's interface, User experience) Интерфейс пользователя
USSD	(Unstructured supplementary service data) Сервис в сетях GSM для передачи коротких сообщений между абонентом сети и сервисным приложением
БВУ/ВУ	Банк второго уровня / внешний участник
БД	База данных

Сокращения

БМР	Банк международных расчетов
ВБ	Всемирный банк
ВЭФ	Всемирный экономический форум
ГУ	Государственное учреждение
ИБ	Информационная безопасность
МВФ	Международный валютный фонд
НБРК	Национальный Банк Республики Казахстан
НПА	Нормативно-правовой акт
ОС	Операционная система
ПО	Программное обеспечение
ПОД/ФТ	Противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма
РК	Республика Казахстан
СПУ	Сервисный поставщик услуг
ТСП	Торгово-сервисное предприятие
ФО	Финансовые организации
ЦВЦБ	Цифровая валюта центрального банка
ЦРПФТ	Центр развития платежных и финансовых технологий НБРК
ЦБ	Центральный Банк
ЦТ	Цифровой тенге

Резюме

В соответствии с поручением Главы государства НБРК реализовал пилотный проект

В соответствии с поручением Главы государства Национальный Банк Республики Казахстан реализовал пилотный проект «Цифровой тенге» в тесном сотрудничестве с участниками финансового рынка, экспертным сообществом и международными финансовыми организациями. Основные вехи проекта представлены ниже.

В подходах к реализации проекта НБРК руководствовались принципами открытости и транспарентности

В подходах к реализации проекта НБРК руководствовался принципами открытости и транспарентности. Каждая стадия проекта сопровождалась публичными обсуждениями, ключевые архитектурные решения принимались с учетом позиций всех заинтересованных сторон и передового международного опыта. За время реализации проекта проведено более 100 встреч различного уровня с участниками рынка, международными экспертами и зарубежными регуляторами.

Технологический потенциал ЦТ позволяет адресовать новые вызовы финансовой стабильности

Ключевой мотивацией в изучении ЦТ послужил его потенциал в улучшении финансовой инклюзивности, развитии конкуренции и инноваций в индустрии платежей, а также повышении конкурентоспособности финансового сектора Казахстана на глобальном рынке. Также новые функциональные возможности платформы ЦТ дополняют существующие платежные системы. Технологический потенциал ЦТ позволяет адресовать новые вызовы финансовой стабильности, включая активное развитие индустрии цифровых активов и децентрализованных финансов.

По итогам проведенных исследований принято решение о необходимости внедрения ЦТ

В целях систематизации исследования была разработана Модель принятия решений о необходимости внедрения ЦТ, учитывающая всестороннюю оценку рисков и преимуществ выпуска национальной цифровой валюты. Для объективного анализа сформирован Консультативный совет из независимых международных и казахстанских экспертов. Серия исследований включила в себя широкий инструментарий: от проведения технологического пилотного проекта до опроса населения. По итогам проведенных исследований принято решение о необходимости внедрения ЦТ. Вместе с тем, с учетом необходимости технологических доработок, подготовки инфраструктуры, проработки операционной модели и нормативно-правовой базы рекомендуется обеспечить поэтапное внедрение за три года. При этом ЦТ должен быть доступен для реальных расчетов уже с 2023 года с поэтапным расширением функциональных возможностей и введением в промышленную эксплуатацию до конца 2025 года.

Рекомендуется обеспечить поэтапное внедрение за три года



[Доклад для публичных обсуждений](#)

[Ответы на вопросы участников обсуждения доклада](#)



[Модель принятия решения](#)

АПРЕЛЬ
2021

МАЙ
2021

ДЕКАБРЬ
2021

ИЮЛЬ
2022

ОКТАБРЬ
2022



[Доклад о результатах исследования](#)



[Пилотный проект с реальными потребителями и торгово-сервисными предприятиями](#)

ЦИФРОВОЙ ТЕНГЕ ОТКРЫВАЕТ ШИРОКИЙ СПЕКТР НОВЫХ ВОЗМОЖНОСТЕЙ ДЛЯ КАЗАХСТАНЦЕВ



Безналичная оплата без доступа к Интернету



Новые финансовые сервисы благодаря программируемости токенов



Расширение доступности финансовых услуг



Удобные взаиморасчёты с государством без угрозы конфиденциальности



Цифровой тенге будет доступен через существующие интерфейсы



Повышенная безопасность и сохранность денежных средств с высоким уровнем анонимности



Безопасные расчеты в сфере цифровых активов и децентрализованных финансов



Круглый стол в Сенате

Внедрение национальной платежной системы. Цифровой тенге – ожидаемые результаты и перспективы развития



Установочная встреча с участниками рынка



Участие в воркшопах МВФ и ВБ по ЦВЦБ

Сообщество практиков и технических специалистов



Региональная конференция стран тропической Африки по ЦВЦБ и криптоактивам



Digital Bridge 2022

Панельная сессия: ЦВЦБ: стратегия и цели внедрения



CordaCon 2022

Более 1000 мировых лидеров финансовых услуг, технологов и энтузиастов Corda от ЦВЦБ до DeFi



Совместный семинар Национального банка Польши и Швейцарского национального банка

Цифровые финансы



X Конгресс финансистов Казахстана

Роль финансовой отрасли в развитии реального сектора: вызовы и возможности

ФЕВРАЛЬ

МАРТ

АПРЕЛЬ

МАЙ

ИЮНЬ

АВГУСТ

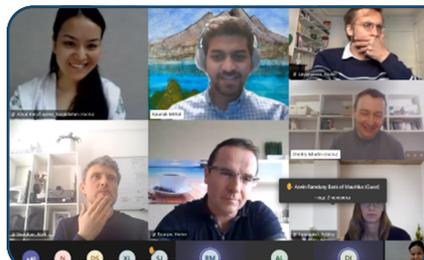
СЕНТЯБРЬ

ОКТАБРЬ

НОЯБРЬ

Встреча с технической группой МВФ и ВБ

Презентация технологических аспектов проекта Цифровой тенге



Q&A сессия с экспертным сообществом и лидерами общественного мнения

Вопросы реализации проекта Цифровой тенге

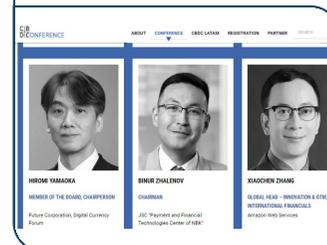


Открытие диалоговой площадки Digital Tenge Hub



Astana Finance Days

Цифровой тенге и глобальный опыт реализации проектов ЦВЦБ



Международная конференция о ЦВЦБ во Франкфурте

42 ЦБ, 190 делегатов из 50 стран мира



Саммит ЦВЦБ 2022 Вашингтон

Мастер-классы, встречи по ЦВЦБ в сотрудничестве с МВФ и другими ЦБ

Вебинар Генерального совета по исламским банкам и финансовым институтам

ЦВЦБ: как они обеспечивают безналичное общество и стабильность финансовой системы



Совместный вебинар НБРК и МВФ о ЦВЦБ

ПАРТНЕРЫ



ОБСУЖДЕНИЯ С ЦБ МИРА



МЕМОРАНДУМЫ



ОХВАТ В СМИ

За 2022 год более

- 50 интервью и письменных комментариев
- 10 видеоинтервью и прямых эфиров на казахстанских телеканалах и зарубежных онлайн площадках
- 5 статей в профильных журналах
- 1483 публикаций
- 2 млн просмотров

Введение

Цифровой тенге – третья форма расчета, которая будет использоваться наряду с наличными и безналичными средствами. ЦТ обладает свойствами существующих форм расчета и открывает новые преимущества для всех участников делового оборота. Цифровой валютой можно расплачиваться точно так же, как и безналичными средствами – через интернет-эквайринг, мобильные приложения, POS-терминалы, QR-коды и т.д.

При этом так же, как и наличные деньги, ЦТ является обязательством НБРК. Поэтому расчеты в ЦТ не несут риски финансовых посредников. В ЦТ можно расплачиваться без доступа к Интернету, в том числе в формате peer-to-peer (с устройства на устройство).

При переводах и платежах с безналичными средствами пользователи не чувствуют отложенную финализацию расчетов межбанковской инфраструктуры. Но в скорости и процессе финализации расчетов в ЦТ имеются отличия. Расчеты в ЦТ завершаются мгновенно и окончательно подобно транзакциям в наличных. При передаче токенов с устройства покупателя на устройство продавца происходит перевод денежной ценности по аналогии купюр без финансового посредничества.

Расчеты в ЦТ более анонимны по сравнению с традиционными безналичными инструментами, а в отдельных сценариях использования конфиденциальность расчетов сопоставима с наличными деньгами. ЦТ предоставляет возможность пользователю скрывать данные от других участников системы, кроме банка – открывателя кошелька. При открытии кошелька пользователь дает доступ к своим данным банку для соответствия правилам ПОД/ФТ. При этом предусмотрена возможность открытия кошельков с упрощенным идентификатором в соответствии с концепцией риск-ориентированного надзора ПОД/ФТ.

К уникальным преимуществам национальной цифровой валюты относятся проведение цепочки транзакций в офлайн-режиме и программируемость. В сравнении с существующими платежными системами ЦТ позволяет проводить несколько транзакций без доступа к Интернету. Текущие карточные системы ограничены одной транзакцией в режиме офлайн, после которой необходимо синхронизировать данные в общем реестре с помощью подключения к сети. Программируемость ЦТ позволяет наделять цифровые деньги особыми свойствами: целевым назначением, адресностью и т.д. без угрозы конфиденциальности транзакций. Например, настраивать доступ к данным транзакции – скрывать отдельные данные транзакции, создавать смарт-контракты – записывать бизнес-логику сценария для автоматизации процесса и исключения посредников.

Новые преимущества ЦТ реализуются за счет гибридной технологии, которая включает централизованные элементы существующих платежных систем и децентрализованные элементы распределенного реестра.

При изучении внедрения ЦТ в экономику обсуждались вопросы технологической реализуемости и надежности, экономического эффекта от внедрения, развития соответствующей экосистемы, а также операционной модели и регулирования платформы ЦТ. Все направления изучались поэтапно, с учетом мнения всех заинтересованных сторон и передового международного опыта.

В 2021 году НБРК запустил исследование возможности внедрения ЦТ в тесном сотрудничестве с участниками финансового рынка, экспертным сообществом и международными партнерами. В ходе исследования были определены свойства ЦТ – параметры модели ЦВЦБ для Казахстана и экспериментально оценена технологическая

жизнеспособность концепции ЦТ на базе технологии распределенного реестра. Была выработана первичная модель оценки влияния ЦТ на экономику, финансовую стабильность и денежно-кредитную политику, а также изучены возможные подходы к регулированию.

В 2022 году НБРК продолжил исследование, а также расширил список аспектов для изучения:

1. **Технология** – технологическая реализуемость свойств ЦТ для достижения целей и задач внедрения
2. **Экономика** – оценка потенциальных выгод и рисков от внедрения ЦТ
3. **Экосистема** – оценка готовности рынка использовать, внедрять ЦТ
4. **Операционная модель** – анализ возможных вариантов взаимодействия участников системы
5. **Регулирование** – анализ правового регулирования ЦТ

Для систематизации вышеописанных аспектов при оценке необходимости внедрения ЦТ была разработана Модель принятия решений. НБРК разработал собственный подход к оценке всех выгод и рисков от запуска ЦТ, который учитывает цели и задачи развития Национальной платежной системы Казахстана.

С учетом рекомендаций ведущих международных финансовых организаций (МВФ, ВЭФ) в казахстанской модели принятия решений были определены все направления, которые необходимы для всестороннего анализа внедрения национальной цифровой валюты.

Анализ опыта стран, реализующих аналогичные проекты, и государств, уже запустивших проекты ЦВЦБ, позволяет сделать ряд выводов.

Принятие решения о дальнейшей работе над ЦВЦБ зависит от изначальных целей и задач, поставленных ЦБ, которые зависят от типа ЦВЦБ, уровня развития экономики страны и

стадии внедрения/изучения. На процесс принятия решения влияют сроки изучения и внедрения ЦВЦБ, а также выбор приоритетных компонентов реализации цифровой валюты. Например, приоритизация изучения технологии либо экономических аспектов на начальном этапе.

Наиболее успешные проекты цифровой валюты могли иметь изначально фундаментальную цель, которая достигалась в ходе экспериментов и пилотных проектов, и далее внимание уделялось другим аспектам (Швеция). Либо, как это было при реализации других проектов, исходили из достаточно простых KPI (например, количество конечных пользователей), но в ходе дальнейшей работы эти показатели пересматривались под воздействием внешних факторов (страны Восточно-карибского бассейна).

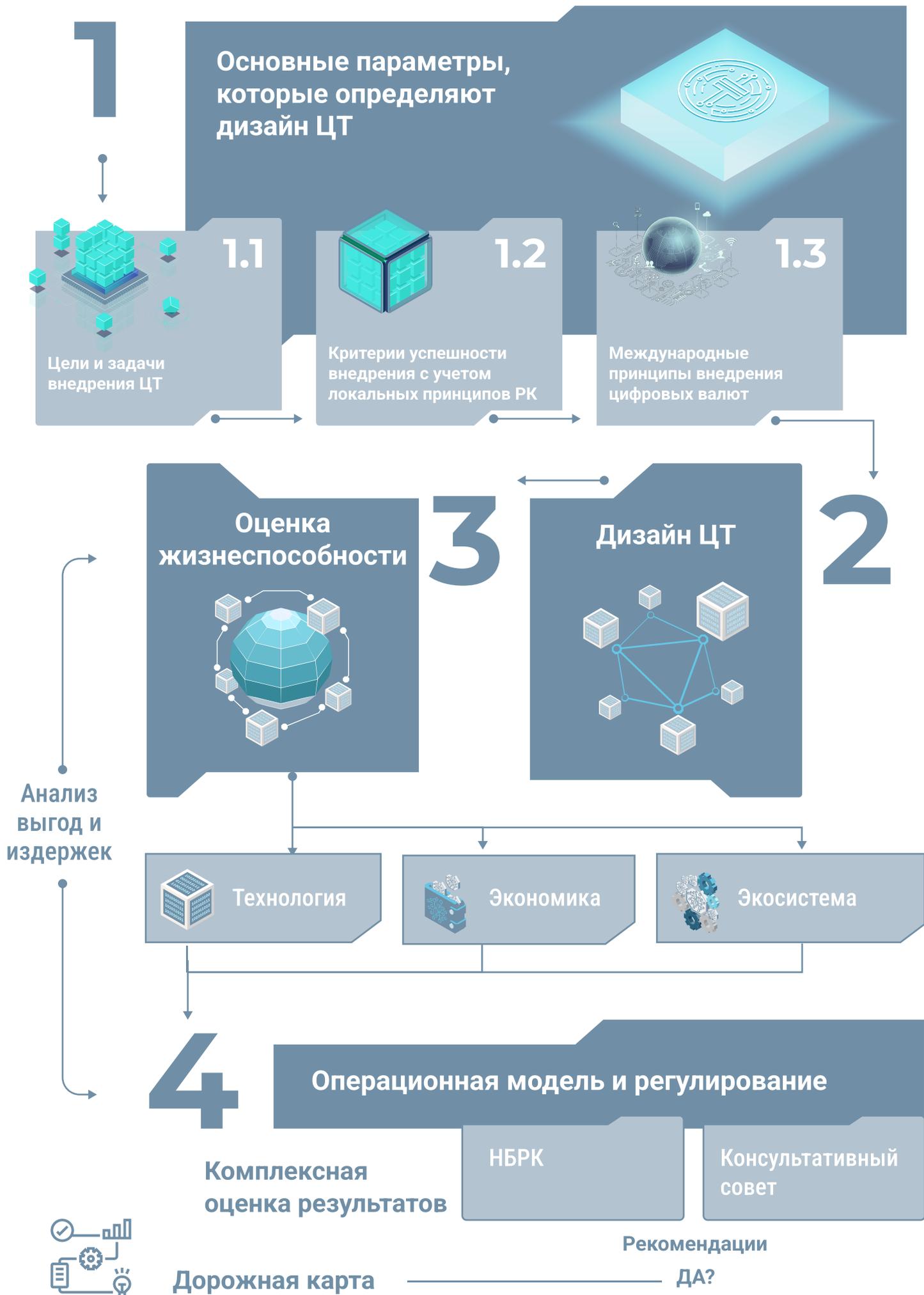
Не существует единой модели принятия решения: различные мотивационные факторы, разные сроки реализации, подходы и стратегии ЦБ.

Для выработки взвешенного решения ключевую роль играет вовлечение участников рынка. Для этих целей НБРК с начала проекта обеспечивает открытые коммуникации с рынком, предоставив площадку для взаимодействия всех заинтересованных сторон.

Структура модели принятия решения – структура документа

Модель принятия решения состоит из основных четырех блоков, согласно которым в данном докладе описаны все итоговые результаты.

1. Основные параметры, которые определяют дизайн ЦТ
2. Определение дизайна ЦТ
3. Экспериментальная оценка жизнеспособности выбранного дизайна ЦТ
4. Концептуальный анализ операционной и регуляторной моделей ЦТ



3

Оценка жизнеспособности



 **Технология**

 **Экономика**

 **Экосистема**

Критерии принятия решения

- 01 Технологический эффект
- 02 Технологические риски и киберриски
- 03 Экономический эффект
- 04 Экономические риски
- 05 Готовность рынка и потребителей

4

Операционная модель и регулирование

- 06 Оценка регуляторного воздействия
- 07 Оценка выгод и издержек в рамках операционной модели

Комплексная
оценка результатов

НБРК

Консультативный
совет



Цели, задачи и принципы внедрения ЦТ

В первой главе настоящего документа представлены **цели, задачи и принципы внедрения ЦТ**. Далее все направления исследования систематизированы в пять блоков:

- 1. Технология**
- 2. Экономика**
- 3. Экосистема**
- 4. Операционная модель**
- 5. Регулирование**

Дизайн ЦТ формируется в контексте каждого

направления. Например, в части технологии определены функциональные и нефункциональные требования к платформе исходя из целей и задач внедрения ЦТ. В свою очередь, экономический дизайн сформирован согласно принципам внедрения ЦТ.

В каждом блоке рассмотрены вопросы и гипотезы исследования. С учетом специфики вопросов выработаны подходы к оценке, также резюмированы основные результаты и выводы изучения каждого направления.

Цели	Возможности ЦТ для достижения целей
1 Повышение конкуренции на финансовом рынке внутри страны	ЦТ предоставит рынку возможности для создания новых продуктов и бизнес-моделей за счет программируемости, смарт-контрактов и безопасной интеграции с открытыми протоколами DLT.
2 Увеличение проникновения безналичных платежей	ЦТ сделает безналичные платежи доступнее в местах с ограниченным доступом к Интернету благодаря цепочке транзакций в офлайн-режиме.
3 Обеспечение бесперебойности функционирования Национальной платежной системы	Новые функциональные возможности ЦТ дополняют действующие платежные системы. В шоковых сценариях ЦТ обеспечивает бесперебойное функционирование Национальной платежной системы.
4 Увеличение эффективности платежей с участием государства	ЦТ повысит эффективность расходования государственных средств без ущерба анонимности граждан. ЦТ дает возможность балансировать между адресностью и анонимностью платежей: целевое использование «маркированных» токенов с возможностью автоматической «обратной маркировки» для обеспечения анонимности последующих транзакций.
5 Повышение конкурентоспособности финансового рынка	Бесшовная интеграция ЦТ с цифровыми платформами внутри страны дает возможность для создания новых платежных и финансовых продуктов. Например, расчет сделок в режиме "поставка против платежа". Также ЦТ ускорит и удешевит трансграничные и оптовые платежи за счет сокращения посредников и использования смарт-контрактов. В контексте глобальных вызовов ЦТ может стать инструментом регулирования и мониторинга транзакций традиционных и децентрализованных финансов за счет токенизации, интеграции с другими системами DLT.

В перспективе внедрение ЦТ обеспечит готовность казахстанского финансового рынка к новым вызовам.

Большинство ведущих торговых партнеров Казахстана находятся на стадии активного внедрения национальных цифровых валют. С учетом тренда на фрагментацию глобальной финансовой инфраструктуры, трансграничные расчеты в ЦВЦБ могут стать критическим элементом торгово-финансовой инфраструктуры. Важно обеспечить готовность Национальной платежной системы к данному сценарию.

Несмотря на так называемую «криптозиму», индустрия цифровых активов и токенизация в финансах продолжают развиваться, а регуляторы крупных юрисдикций вырабатывают соответствующие подходы к регулированию, включая пруденциальное регулирование «стейблкоинов», обеспеченных фиатными валютами. Данные тренды приведут к росту популярности их использования в качестве платежного средства в онлайн. Неконтролируемое распространение цифровых активов среди казахстанских потребителей чревато рисками «криптоизации» – возможного перетока ликвидности с текущих счетов и депозитов в обеспеченные мировыми резервными валютами стейблкоины.

Благодаря использованию технологии распределенного реестра, ЦТ может стать дополнением к традиционной финансовой инфраструктуре, которая, с одной стороны, обеспечивает защиту прав потребителей и макро- и финансовую стабильности от вышеуказанных рисков, с другой стороны, сохраняет возможность использования инновационного потенциала цифровых активов.

Локальные и международные принципы внедрения ЦТ

В отличие от подходов других ЦБ в Казахстане особое внимание уделяется естественному стимулированию интереса рынка к ЦТ. К локальным принципам внедрения относятся:

1. Естественное развитие интереса рынка к использованию ЦТ, а также созданию новых сервисов и продуктов с ЦТ без применения административно-командных методов.
2. Обеспечение равного доступа к системе ЦТ.
3. Ориентированность на покупателя – защита интересов потребителей.

Вдобавок при формировании бизнес-требований к ЦТ учтены международные принципы внедрения ЦВЦБ. Принципы G7 являются продолжением базовых принципов БМР:

1) Основопологающие принципы внедрения ЦВЦБ

- наличие юридических и регуляторных рамок
- защита данных
- сосуществование с существующими платежными системами
- операционная устойчивость и кибербезопасность
- препятствование противозаконной финансовой деятельности
- стабильность международной монетарной и финансовой систем
- экологичное использование

2) Дополнительные возможности ЦВЦБ

- поддержка инноваций в цифровой экономике
- повышение финансовой инклюзивности;
- платежи в государственном секторе
- кросс-граничные платежи
- поддержка развития международного сотрудничества

ТЕХНОЛОГИЯ



17-49
стр.

Дизайн ЦТ

Ключевая цель проекта на 2022 год с точки зрения технологии – исследование аспектов внедрения ЦТ, тестирование расширенной функциональности технологической платформы

Ключевая цель проекта на 2022 год с точки зрения технологии – исследование аспектов внедрения ЦТ, тестирование расширенной функциональности технологической платформы на базе ранее разработанного прототипа. Реализация проекта 2022 года служит основой для принятия решения о необходимости внедрения ЦТ в Республике Казахстан.

На основе целей и задач проекта, а также с учетом международной экспертизы были определены ключевые гипотезы для проверки в рамках пилотного проекта. На основании ключевых гипотез для реализации в проекте были сформулированы функциональные и нефункциональные требования.

Ключевые параметры дизайна ЦТ В Докладе для публичных обсуждений «Цифровой тенге» сформулированы ключевые параметры дизайна ЦТ.

В рамках текущего проекта определены дополнительные параметры дизайна ЦТ

В рамках текущего проекта определены дополнительные параметры дизайна ЦТ: модель открытия кошельков, подход к анонимности, к решению «последней мили».

Ключевые гипотезы для проверки в рамках пилотного проекта

Название гипотезы	Краткое описание
Простота интеграции	<p>Возможность простого подключения внешних участников к платформе</p> <p>Интеграции с мобильными приложениями внешних участников</p> <p>Возможность безопасной интеграции с открытыми протоколами DLT</p>
Сокращение количества посредников	<p>Возможность передавать стоимость напрямую без посредников</p> <p>Токены с ЦТ передаются непосредственно от отправителя к получателю</p>
Офлайн-транзакции	<p>Подтверждение технологической возможности проведения цепочки офлайн-платежей при перебоях в работе интернета или в регионах с недостаточным интернет-покрытием</p> <p>Средства, полученные в офлайне, могут быть использованы далее в офлайне</p>
Настраиваемая анонимность	<p>Возможность настройки анонимности пользователем на уровне транзакции, например, скрывать свои данные во время перевода</p>
Баланс между отслеживаемостью и конфиденциальностью	<p>Возможность отслеживаемости транзакций, в т.ч. в соответствии с требованиями ПОД/ФТ без угрозы анонимности потребителей</p>
Непрерывность функционирования	<p>Отсутствие единой точки отказа</p> <p>Обеспечение бесперебойности работы</p> <p>Возможности совершения транзакций 24/7</p>
Программируемость	<p>Функционал по обеспечению целевого расходования и адресности средств путем программирования токена</p> <p>Например, встраивание в токен информации о его типе для отслеживания целевого использования</p>
Интероперабельность	<p>Возможность обеспечения эффективного взаимодействия с другими платежными системами</p>
Безопасность транзакций	<p>Транзакции с использованием ЦТ как минимум не уступают транзакциям с использованием безналичных средств по уровню информационной безопасности и конфиденциальности</p>

Соответствие задач внедрения ЦТ в Казахстане и гипотез проекта

Задача модели принятия решения / Гипотеза	Повышение конкуренции на финансовом рынке внутри страны	Увеличение проникновения безналичных платежей	Обеспечение бесперебойности функционирования Национальной платежной системы	Увеличение эффективности платежей с участием государства	Повышение конкурентоспособности финансового рынка по отношению к игрокам из разных секторов экономики и других стран
--	---	---	---	--	--

Простота интеграции	▼	▼	▼	▼	▼
Сокращение количества посредников	▼	▼	▼	▼	▼
Офлайн-транзакции	▼	▼	▼		▼
Настраиваемая анонимность	▼	▼		▼	▼
Отслеживаемость	▼	▼		▼	▼
Непрерывность функционирования	▼	▼		▼	▼
Программируемость	▼	▼		▼	▼
Интероперабельность	▼	▼	▼	▼	▼
Безопасность транзакций	▼	▼	▼	▼	▼

▼ *основной эффект*

▼ *дополнительный эффект*

На основании ключевых гипотез для реализации в проекте были сформулированы функциональные и нефункциональные требования.

Функциональные требования

Функциональные требования были заложены в функциональность сценариев. Перечень сценариев включает следующие типы:

- Базовые сценарии MVP – базовые сценарии жизненного цикла ЦТ (от эмиссии до обращения).
- Сценарии MVP с расширенной функциональностью – сценарии с ЦТ специального назначения, сценарий перевода с использованием QR, перевыпуск и мониторинг.
- Сценарий R&D – сценарий для тестирования инновационных свойств ЦТ (офлайн-транзакции).

Сценарии MVP и R&D

БАЗОВЫЕ СЦЕНАРИИ MVP

Открытие кошельков БВУ и ВУ / ГУ

Открытие кошельков для ФЛ

Открытие кошельков для ТСП

Эмиссия и распределение БВУ и ВУ / ГУ

Распределение клиентам (стандартные ЦТ)

C2C перевод (по номеру мобильного телефона)

Покупка в онлайн-режиме за стандартные ЦТ

СЦЕНАРИИ MVP С РАСШИРЕННОЙ ФУНКЦИОНАЛЬНОСТЬЮ

Маркировка токенов

Распределение специальных ЦТ клиентам

Покупка за специальные ЦТ

C2C перевод (по QR)

Перевыпуск (вкл. техническое погашение)

Мониторинг

СЦЕНАРИИ R&D

Офлайн-платежи (с цепочкой офлайн-транзакций)

Сценарий внешнего участника (BTS): оплата за проезд

Сценарии внешнего участника (Евразийский Банк): открытие кошелька, перевод, покупка

При разработке платформы в 2022 году одним из важных функциональных требований стала **независимость от вендора** – поставщика технологии (независимость от лицензии, от доработок на стороне вендора). Для реализации цели по обеспечению технологической независимости Казахстана в ходе проекта было использовано ПО с открытым исходным кодом.

Нефункциональные требования

На основании ожидаемых результатов разработки ПО платформы ЦТ (MVP и R&D), ключевых гипотез и требований к

Ключевые гипотезы для проверки в рамках пилотного проекта

Гипотеза	Название гипотезы	Краткое описание
Непрерывность функционирования	Наблюдаемость	Предусмотрена возможность логирования (отслеживание статуса работы системы и ее компонентов), а также технического мониторинга инфраструктуры MVP пилотной платформы
	Послеаварийное восстановление	Предусмотрены механизмы резервного копирования и восстановления данных из резервных копий для продуктивной среды MVP пилотной платформы. Предусмотрено ручное восстановление БД в случае аварии из резервных копий
	Доступность	Доступность MVP пилотной платформы составляет 95% в период пилотирования, максимальное время недоступности – 1 час в день (в случае обновлений системы)
Офлайн-транзакции	Каналы связи	В архитектуре для направления R&D ПО пилотной платформы предусмотрена возможность совершения операций через мобильные устройства без доступа либо с ограниченным доступом к сети Интернет. При появлении доступа транзакции, совершенные в офлайн-режиме, синхронизируются и таким образом интегрируются в общую историю транзакций
Простота интеграции	Интеграция с внешними участниками	Интеграция с внешними участниками реализуется с помощью методов REST API, общепринятого способа предоставления API, используемого в любом языке программирования и поддерживаемого многочисленными библиотеками

инфраструктуре были сформулированы требования в части нефункциональных аспектов платформы ЦТ, которые могут быть проверены аналитически или практически.

Требования, проверяемые практически: предположения, которые могут быть экспериментально подтверждены или опровергнуты после реализации Сценария в рамках пилотного проекта или в рамках нагрузочного тестирования.

Ключевые гипотезы для проверки в рамках пилотного проекта

Гипотеза	Название гипотезы	Краткое описание
Интероперабельность	Совместимость с международными стандартами в части QR	Разработка требований к QR с учетом существующего национального стандарта СТ РК 3712-2021 [9] (требования к составу данных QR-кода для приема платежей), а также международного стандарта ISO 18004 [3] (спецификация символики QR-кода)
	Совместимость с международными стандартами в части передачи финансовых сообщений	Формирование спецификаций API и разработка API пилотной платформы ЦТ с учетом потенциальной применимости платежных стандартов ISO 20022 [2]
Технические требования (не относятся ни к одной из гипотез)	Пропускная способность	Замеры пропускной способности на нагрузке пилотного проекта
	Длительность обработки транзакции	Средняя длительность транзакций в пилотном проекте составляет не более 5 сек. Длительность транзакций покупок и переводов в части corda транзакции, API интеграции и отображения в банковском фронт-енде составляет не более 15 сек.

Требования, проверяемые аналитически: предположения, которые могут быть экспериментально подтверждены или опровергнуты только на этапе опытной эксплуатации платформы. Практическое тестирование данных задач лежит вне рамок пилотного проекта, данные требования проверены аналитическим способом.

Перечень задач, проверяемых аналитически в рамках пилотного проекта

Гипотеза	Название гипотезы	Краткое описание
Непрерывность функционирования	Возможность переноса на другую инфраструктуру	Платформа обладает возможностью переноса на другую инфраструктуру без необходимости вносить кардинальные изменения в архитектуру и функциональность платформы
	Масштабируемость	В архитектуре MVP пилотной платформы заложена возможность масштабирования ресурсов (вертикальная масштабируемость) для обеспечения бесперебойной работы при высоких нагрузках, а также возможность дальнейшего увеличения числа пользователей и развертывания в масштабах национальной платёжной системы за счет горизонтального масштабирования

Перечень задач, проверяемых аналитически в рамках пилотного проекта

Гипотеза	Название гипотезы	Краткое описание
Простота интеграции	Интеграция с открытыми протоколами DLT	В архитектуре MVP пилотной платформы заложена возможность интеграции с другими платформами на базе распределенного реестра. Одним из способов построения интеграции может быть создание технологических мостов.

Требования в части информационной безопасности

На основании ожидаемых результатов разработки ПО платформы ЦТ (MVP и R&D), ключевых гипотез и требований к инфраструктуре были сформулированы требования и гипотезы относительно аспектов информационной безопасности платформы ЦТ, которые могут быть проверены практически.

Требования, проверяемые практически: предположения, которые могут быть экспериментально подтверждены или опровергнуты после прохождения Сценария в рамках пилотного проекта или в рамках нагрузочного тестирования.

Перечень требований, проверяемых технически в рамках пилотного проекта

Гипотеза	Название гипотезы	Краткое описание
Безопасность транзакций	Идентификация и аутентификация	В MVP пилотной платформы обеспечивается идентификация и аутентификация пользователей и процессов, запускаемых от имени пользователей, а также процессов, запускаемых от имени системных учетных записей
	Ролевая модель	Доступ к чтению и редактированию данных MVP пилотной платформы ограничен с помощью реализации ролевой модели доступа
	Управление инцидентами ИБ	Реализован процесс управления инцидентами ИБ. Мониторинг и обнаружение инцидентов осуществляется при помощи наблюдений или технических средств
	Криптографические механизмы защиты информации	Применяются алгоритмы шифрования с использованием протоколов TLS и SSH. Хранимые пароли доступа к базе данных защищены с помощью алгоритма шифрования SHA-512. Применяются асимметричные алгоритмы криптографии (криптография на эллиптических кривых): алгоритмы подписи и проверки подписи, создания одноразовых stealth-адресов и одноразовых приватных ключей к ним, скрывание сумм с помощью обязательства Педерсена.

Целевая архитектура платформы ЦТ

Потенциальная целевая функциональная архитектура для розничной ЦТ может иметь следующее функциональное наполнение:

- Ядро платформы ЦВЦБ с бизнес-логикой и инструментами интеграции и управления платформой;
- Интегрируемые фронтальные решения и сервисные приложения участников платформы;
- Подключение к системам национального уровня;
- Интероперабельность с другими DLT системами, в том числе в рамках платформ DeFi.

Целевая платформа является критически важной для жителей РК, необходимо реализовать усиленные меры защиты, способные сохранить денежные средства, а также финансовую стабильность РК. Для этого в **целевой платформе необходимо:**

- Обеспечить возможность самостоятельного сопровождения, развития и масштабирования платформы без сторонних вендоров или поставщиков услуг
- Обеспечить разработку платформы с учетом всех необходимых технических средств, принципов и практик в области ИБ
- Реализовать сетевую защиту платформы и каналов связи
- Обеспечить управление доступом и правами к платформе
- Реализовать антивирусную защиту информации
- Осуществить мониторинг, обнаружение и реагирование на инциденты ИБ;
- Обеспечить управление привилегированным доступом, а также доступом подрядчиков
- Реализовать защиту данных от утечек
- А также внедрить иные другие меры ИБ на основе рисков и лучших практик в области ИБ

Подход к выбору целевого технологического решения

Одним из ключевых вопросов на последующих этапах проекта стал выбор целевой технологии распределенных реестров. Существуют варианты использования готового решения, разработанного вендором (коробочное решение), а также ПО с открытым исходным кодом.

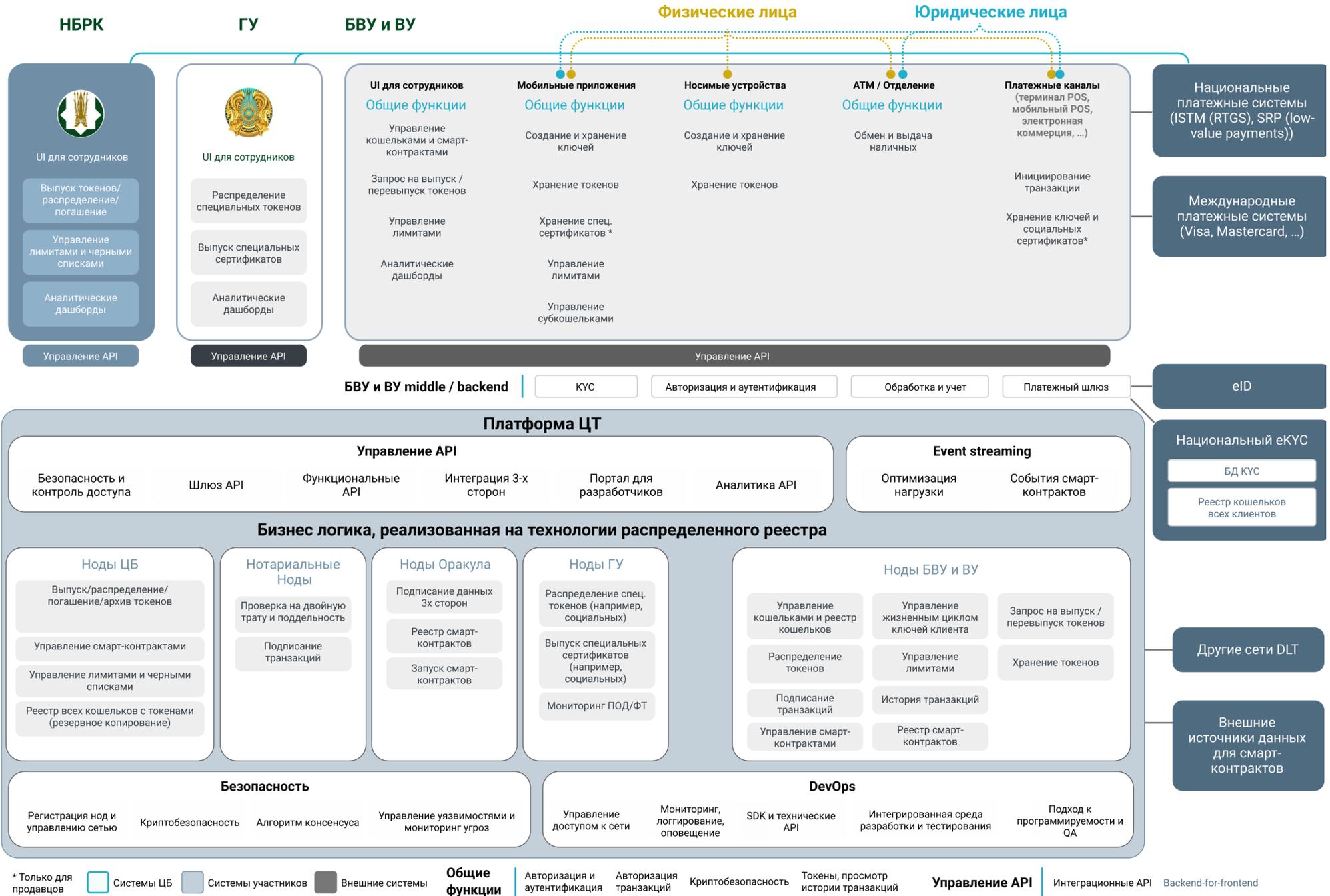
Основываясь на модели принятия решений [8], а также продолжая разработку PoC, было принято решение о том, что технологической базой для направлений MVP и R&D будет платформа Corda R3 Community Edition, так как она удовлетворяет требованиям, сформированным для данного этапа проекта.

По результатам проведенного тестирования и пилотирования в закрытых тестовых окружениях Corda продемонстрировала допустимые результаты производительности для функционирования сценариев MVP и R&D. Однако приемлемость данной платформы для продуктивного решения должна тестироваться в условиях, приближенных к реальным.

При выборе целевой технологии для ЦТ в Республике Казахстан особое внимание уделялось вендорной независимости, бесперебойности работы системы, а также национальному технологическому суверенитету.

При принятии решения о целевой технологии также учитывалось наличие гибкой целевой архитектуры, которая позволяет реализовывать различные варианты пользовательских сценариев (целевые сценарии будут определены на следующем этапе проекта).

Видение целевой архитектуры платформы ЦТ



* Только для продавцов

Системы ЦБ

Системы участников

Внешние системы

Общие функции

Авторизация и аутентификация

Авторизация транзакций

Криптобезопасность

Токены, просмотр истории транзакций

Управление API

Интеграционные API

Backend-for-frontend

Ключевые архитектурные решения

Ключевые параметры дизайна ЦТ

В Докладе для публичных обсуждений «Цифровой тенге» сформулированы ключевые параметры дизайна ЦТ.

Ключевые параметры дизайна ЦТ

Аспект дизайна	Описание
Безопасность транзакций	В MVP пилотной платформы обеспечивается идентификация и аутентификация пользователей и процессов, запускаемых от имени пользователей, а также процессов, запускаемых от имени системных учетных записей
Гибридная инфраструктура	Комбинация централизованной и децентрализованной систем. Использована платформа распределенных реестров (DLT), позволяющая хранить, управлять и вести учет цифровой валюты и операций с ней. При этом платформа содержит элементы централизованной системы: <ul style="list-style-type: none">• подключение инфраструктурных участников (БВУ/ВУ, госучреждений и т.п.) к платформе обеспечивает НБРК• подключение физических и юридических лиц обеспечивают БВУ/ВУ через открытие цифровых кошельков на платформе ЦТ, предоставляемой НБРК• отсутствие двойной траты, то есть невозможность использования одних и тех же ЦТ в разных операциях, гарантируемое НБРК
Доступ на основе токена	При доступе на основе токена использование средств зависит от способности получателя платежа проверить действительность платежного объекта.
Двухуровневая архитектура	НБРК осуществляет эмиссию цифровой валюты, контроль за безопасностью системы, отвечает за распределенный реестр и устанавливает критерии, которым должны соответствовать участники пилотной платформы. Посредники (коммерческие банки, финтех-организации) осуществляют взаимодействие с конечными пользователями: открытие и обслуживание кошельков клиентов, проведение розничных платежей, КУС.

При проектировании архитектуры ЦТ был использован token-based подход («на основании токена»). Он подразумевает, что ЦВЦБ существует в виде токенов, имеющих определенные номиналы, в распределенном реестре. В рамках транзакций осуществляется передача токенов от пользователя к пользователю. При этом транзакция пройдет успешно, если будет подтверждена валидность используемых в транзакции токенов.

Данный подход дает возможность реализовать ряд дополнительных преимуществ ЦВЦБ:

- программируемость на уровне токена;
- проведение транзакций в офлайн-режиме;
- настраиваемая анонимность.

В рамках **текущего проекта** определены дополнительные параметры **дизайна ЦТ: модель открытия кошельков, подход к анонимности, к решению «последней мили».**

Модель открытия кошельков

На платформе реализован подход к открытию кошельков в соответствии с двухуровневой моделью. Клиенты открывают кошельки в БВУ/ВУ, отвечающих за выполнение требований ПОД/ФТ и КУС. НБРК является оператором пилотной платформы и не участвует в процессе открытия кошельков ФЛ и ТСП.

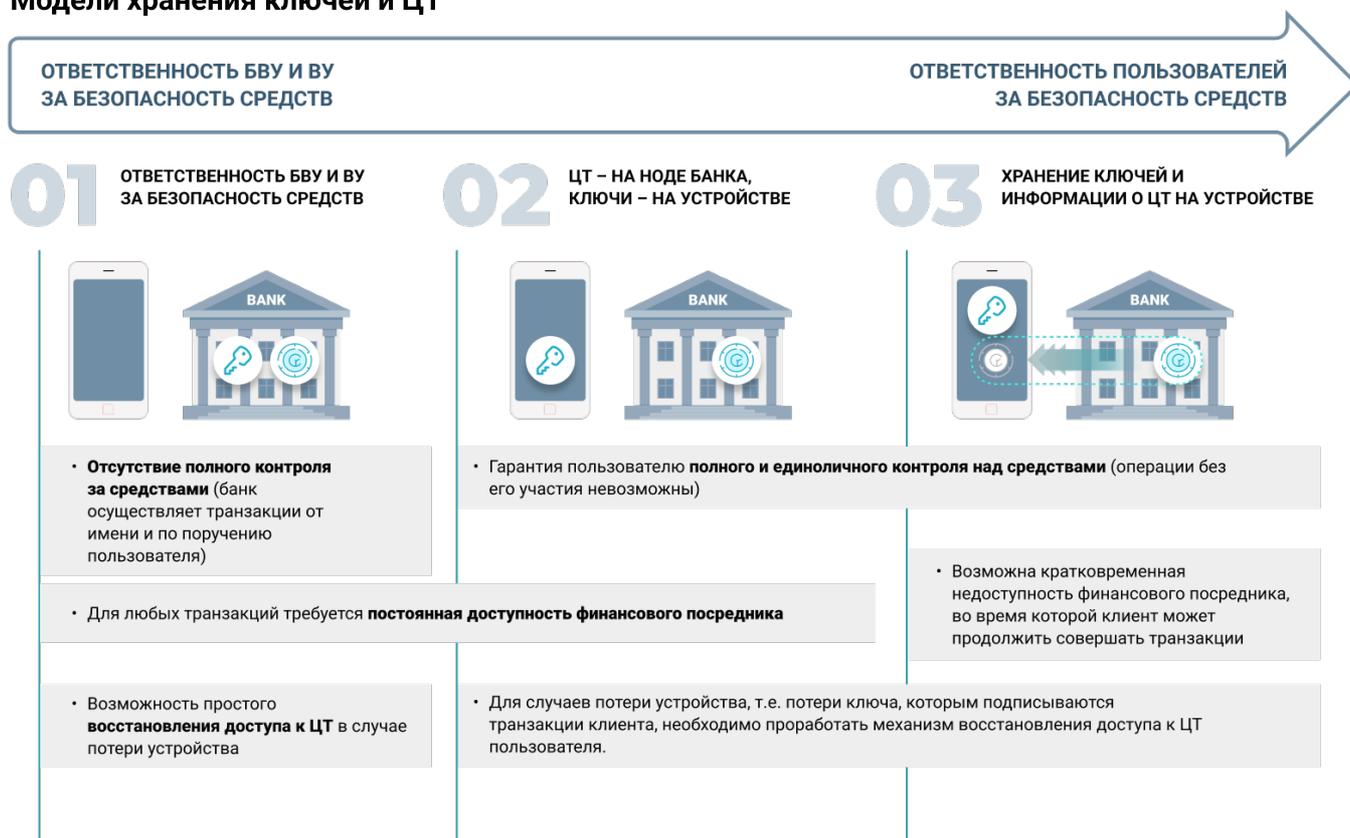
Реализована универсальная модель, при которой возможно открытие нескольких кошельков для клиентов в разных банках (1 банк = 1 кошелек пользователя с разными типами токенов).

Преимуществами выбранной модели являются:

- Повышение конкуренции: один и тот же продукт можно получить у разных провайдеров. У финансовых игроков больше возможностей для конкуренции за клиента за счет свойств продукта;
- Свобода для потребителя: гибкая возможность управления своими деньгами через разные кошельки. Возможность контроля за всеми кошельками в разных БВУ/ВУ через «единое окно» может быть реализована через финтех-сервисы в соответствии с концепцией Открытого Банкинга;
- Защита прав потребителя: нет жесткой зависимости от конкретного БВУ/ВУ. Разные БВУ/ВУ могут реализовывать различные модели хранения ключей. У клиента есть возможность выбора БВУ/ВУ и, соответственно, модели хранения ключей. Таким образом, клиент самостоятельно определяет уровень ответственности, которую он готов нести за безопасность своих средств.

Существует три модели хранения ключей и ЦТ.

Модели хранения ключей и ЦТ



В рамках **первой модели** предусмотрено хранение ключей и ЦТ на ноде БВУ/ВУ (отсутствует передача на устройство клиента информации о ЦТ, заверенной банковской подписью). Модель позволяет клиенту передать ответственность за безопасность средств БВУ/ВУ. В рамках модели транзакции подписывает БВУ/ВУ от имени клиента.

Вторая модель предусматривает хранение ключей на устройстве клиента. Информация о ЦТ, заверенная банковской подписью, не передается на устройство клиента. Данная модель не позволяет БВУ/ВУ использовать средства клиента без его ведома. В рамках этой модели требуется постоянная доступность финансового посредника для совершения операций.

Третья модель предусматривает хранение ключей на устройстве клиента, а также передачу на устройство клиента информации о ЦТ, заверенной банковской подписью. В R&D

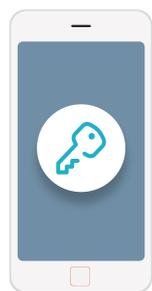
данное действие обозначается как депозит: на кошельке на устройстве клиента появляется информация о токене.

Перед передачей на устройство клиента информация подписывается БВУ/ВУ. При осуществлении клиентом транзакций в офлайн-режиме информация о депозите передается с банковской подписью. Для подтверждения валидности депозита в офлайне подпись может проверить любой другой участник транзакции.

Таким образом, третья модель позволяет производить транзакции в офлайн-режиме, в том числе при недоступности БВУ/ВУ.

Одной из важных задач экспериментального исследования было **тестирование возможности осуществления цепочки офлайн-транзакций**. Таким образом, с точки зрения дизайнера, для офлайн-транзакций была использована Модель 3.

В R&D была протестирована **гибридная модель**, где использованы различные способы хранения ключей и токенов для онлайн и офлайн-кошельков:

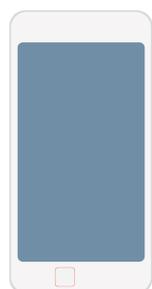


Онлайн-кошелек

кошелек с поддержкой только онлайн-режима

Реализовано в RD и двумя внешними участниками в MVP

— 02



Онлайн-кошелек

кошелек с поддержкой только онлайн-режима

Реализовано одним внешним участником

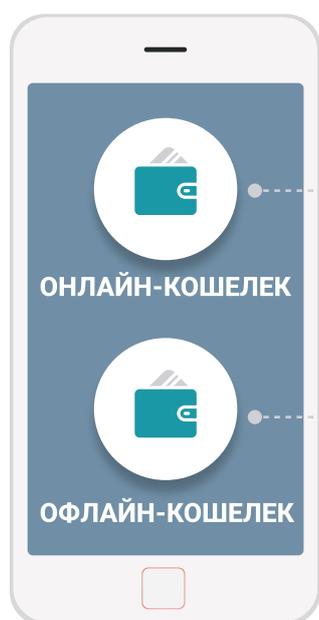
— 01

ГИБРИДНАЯ МОДЕЛЬ:

ОНЛАЙН – ЦТ НА НОДЕ БВУ

ОФЛАЙН – ИНФОРМАЦИЯ О ЦТ НА УСТРОЙСТВЕ ПОЛЬЗОВАТЕЛЯ

КЛЮЧИ – ВСЕГДА НА УСТРОЙСТВЕ ПОЛЬЗОВАТЕЛЯ



— 02



— 03

В рамках данной модели в R&D создается пара кошельков: один кошелек с поддержкой онлайн-режима («онлайн-кошелек», Модель 2), второй кошелек – с возможностью совершения офлайн-транзакций («офлайн-кошелек» или «кошелек на устройстве», Модель 3). **Преимуществом** выбранной гибридной модели является гарантия пользователю единоличного **контроля над средствами** (операции без его участия невозможны), а также **возможность проведения операций в офлайн-режиме**.

Подход к анонимности

В рамках проекта 2022 года реализованы идентифицированные кошельки: БВУ/ВУ, в котором открыты кошельки клиентов и которому известны транзакции своих клиентов.

Реализована логика настраиваемой анонимности, которая предоставляет возможность клиенту быть анонимным для других участников, но не для БВУ/ВУ, в котором открыт кошелек клиента.

В архитектуру решения заложена гибкая модель открытия кошельков, допускающая в будущем возможность принятия решения о типах кошельков (в т.ч. возможности анонимности) и подходу к KYC пользователя.

Модель допускает возможность введения разных типов кошельков в зависимости от уровня идентификации пользователя (например, анонимный в пределах определенных лимитов по сумме, частично идентифицированный, полностью идентифицированный).

Анонимность пользователя

В MVP реализован функционал «настраиваемой анонимности», когда пользователь может самостоятельно выбирать: показывать персональные данные другим пользователям (участникам транзакции) или нет. В случае, когда

отправитель хочет остаться анонимным, только нода может его идентифицировать. Приватный view-ключ позволяет по одноразовому stealth-адресу определить, какому основному публичному адресу, он соответствует. Таким образом, даже если клиент хочет остаться анонимным, банк может обеспечивать требования KYC и ПОД/ФТ.

Скрытие информации в транзакции

Дизайн решения позволяет настраивать различные варианты по скрытию информации в транзакции самим пользователем (например, скрытие суммы транзакции, типа токена, товаров и других параметров). В MVP по умолчанию сумма транзакции скрыта от участников сети (ее знают лишь непосредственные участники).

Отслеживаемость

В модель заложен **различный уровень отслеживаемости** в зависимости от типа ЦТ. По специальным типам ЦТ доступен более детальный уровень аналитики. Так, для органа, выпускающего и отслеживающего целевое использование выпущенных специальных ЦТ, доступна аналитика по использованию данных ЦТ. Таким образом повышается прозрачность использования распределенных средств.

Подход к решению «последней мили»

Одним из критериев успешности внедрения ЦТ является **естественное развитие интереса рынка** к использованию цифровой валюты (включая использование ЦТ в офлайн-платежах). В ходе разработки ЦТ важным решением является определение носителей, которые могут быть использованы для осуществления офлайн-транзакций.

Решения для встраивания офлайн-кошельков в различные носители (классическая проблема «последней мили») могут предлагаться разными рыночными провайдерами (в т.ч. в кооперации с производителями устройств, OS, вендорами

платежной инфраструктуры и ЦВЦБ решений). При этом НБРК как оператор централизованной инфраструктуры ЦТ должен отвечать за выбор, аттестацию и сертификацию таких решений для использования их игроками рынка (включая сертификацию с точки зрения безопасности, с определением модели управления рисками и инцидентами ИБ).

В MVP в качестве ОС для устройства пользователя и мобильного PoS ТСР выбраны ОС Android и iOS.

Архитектура решения

Архитектурный подход

При проектировании архитектуры платформы ЦТ применен эволюционный подход. В модели принятия решения [8] в качестве ключевого технологического функционала указаны **гибкость системы, возможность программирования и реализация офлайн-платежей**. Основываясь на модели принятия решения [8], а также продолжая разработку PoC, технологическим решением для направлений MVP и R&D выбрана платформа **Corda R3 Community Edition** на основе модели UTXO.

Для достижения **гибкости платформы ЦТ и интероперабельности** с различными внешними участниками (ГУ, БВУ, финтех-компания) использован подход **многоуровневой архитектуры**, закладывающий также возможность программируемости ЦТ на различных уровнях (начиная от свойств ЦТ до логики в системах внешних участников).

Интероперабельность платформы ЦТ с иными платежными системами/финансовыми механизмами (биржами, маркетплейсами и др.) поддерживается за счет работы по интеграции стандарта ISO 20022 [2] в интеграционный слой для взаимодействия с платформой ЦТ.

QR-код использовался в сценариях перевода и покупки для передачи реквизитов. Для обеспечения интероперабельности платформы ЦТ в части QR-кода велась работа по определению требований к QR-коду с учетом:

- существующего национального стандарта СТ РК 3712-2021 [9] (требования к составу данных QR-кода для приема платежей),
- международного стандарта ISO 18004 (спецификация символики QR-кода) [3].

Наличие в Казахстане зон со слабым интернет-покрытием представляет значительный риск для проникновения ЦТ во все регионы. **Реализация цепочек офлайн-платежей** стала фокусом R&D этапа, так как оплата без подключения к интернету может стать решением данной проблемы.

Важное значение для принятия решения о выходе в продуктивную эксплуатацию имеют также **технологические риски и стабильность платформы**. В качестве основы для проекта выбрана технология распределенного реестра с контролем доступа к сети новых участников, а также реляционные БД. На базе данных технологий разрабатывается полностью кастомное решение, которое позволяет реализовать необходимые пользовательские сценарии, расширить свойства ЦТ в рамках программируемости, а также настроить ПОД/ФТ мониторинг поверх платформы ЦТ.

Интеграция с внешними участниками

Важным критерием успешности внедрения ЦТ является **обеспечение равного доступа к системе ЦТ**. В ходе проекта была запущена площадка Digital Tenge Hub, куда были приглашены участники рынка для тестирования уникальной функциональности ЦВЦБ. Все участники, проявившие заинтересованность в проекте, участвовали в совместной разработке сценариев, а также проработке идей дальнейшего развития ЦТ.

2022 год был нацелен на тестирование работы с реальными мобильными приложениями внешних участников, а также тесное взаимодействие с внешними участниками по развитию платформы (проработка пилотных сценариев, обучение разработкам на базе технологии распределенного реестра и проверка R&D гипотез в песочнице платформы ЦТ).

В рамках MVP-направления осуществлена **интеграция с мобильными приложениями**, разрабатываемыми внешними участниками (банками второго уровня, финтех-компаниями).

На стороне внешних участников находилось и **подключение разработанных мобильных интерфейсов к платформе ЦТ через интеграционный слой** (для взаимодействия с пользователями и инициации транзакций) API.

Первым этапом к построению целевой API management платформы для расширенного управления доступом к платформе ЦТ стало **внедрение контроля доступа к платформе на уровне приложений** через индивидуальные API key, а также на уровне доступа сотрудников к определенным данным на базе ролевой модели.

Для подготовки к проведению пилотного проекта внешние эксперты принимали активное участие в обучении участников пилотного проекта (ТСП и физических лиц),

организации процесса поддержки пользователей в ходе проведения тестирования результатов MVP в рамках пилотного проекта.

Реализованные внешними участниками приложения использовались пользователями в ходе проведения пилотирования платформы ЦТ (подробнее результаты пилотирования приведены в разделе 3.4).

В рамках R&D направления была создана отдельная **технологическая песочница для проведения экспериментов**, развернутая как отдельная среда, на кодовой базе, реализованной в направлении MVP.

Гипотезы и вопросы исследования

Основной целью пилотного проекта на 2022 год являлось тестирование расширенной функциональности ЦТ, пилотирование ЦТ на реальных пользователях, экспериментальная проверка инновационных свойств ЦТ.

Среди ключевых вопросов технологического решения в рамках пилотного проекта можно выделить:

1. Анализ возможностей программирования.

Реализация и тестирование программируемости ЦТ совместно с внешними участниками, а именно возможность задания ограничений по использованию ЦТ в структуре токена для упрощения отслеживаемости целевого использования ЦТ.

2. Возможность осуществления цепочки офлайн-транзакций.

Подтверждение технологической реализуемости нескольких транзакций при отсутствии интернет-соединения у отправителя и получателя средств.

3. **Легкость интеграции.** Подтверждение возможности легкого подключения внешних участников к платформе, реализация интеграции с мобильными приложениями внешних участников, а также возможность разработки собственных сценариев внешними участниками в технологической песочнице.

4. **Реализация настраиваемой анонимности.** Возможность настройки анонимности на уровне транзакции (по усмотрению пользователя).

5. **Возможность использования ЦТ как средство платежа.** Тестирование возможности совершения оплаты и переводов с использованием ЦТ реальными пользователями.

6. **Оптимизация производительности.** В том числе за счет реализации функционала технического погашения и замены старого токена с длинной цепочкой транзакций на новый без истории.

Подход к оценке

В части оценки технологических аспектов на 2022 год определены следующие подходы:

- пилотирование сценариев жизненного цикла в условиях, приближенных к реальным (в замкнутом опытном контуре с ограниченным числом участников);
- экспериментальное исследование передовых и инновационных функциональных возможностей и сервисов использования цифровых валют (таких как цепочка офлайн-транзакций);
- вовлечение внешних участников в проект для совместной выработки видения этапов внедрения ЦТ в Казахстане.

Краткое описание сценариев MVP и R&D

№	Сценарий	Подтвержденные гипотезы	Краткое описание сценария
1	Открытие кошельков БВУ/ВУ или госучреждения	Простота интеграции	Первоначальное создание цифрового кошелька инфраструктурного участника второго уровня (БВУ/ВУ или госучреждения) для работы с ЦТ.
2	Открытие кошельков для физических лиц	Простота интеграции	Первоначальное создание цифровых кошельков для клиентов БВУ/ВУ – физических лиц. Открытие кошельков осуществляется только через аккредитованные (участником первого уровня – НБРК) организации.
3	Открытие кошельков для ТСП	Простота интеграции	Первоначальное создание цифровых кошельков для клиентов БВУ/ВУ – ТСП. Открытие кошельков осуществляется только через аккредитованные (участником первого уровня – НБРК) организации.
4	Эмиссия и распределение БВУ/ВУ или гос. учреждению	Безопасность транзакций	Первоначальное создание токенов ЦТ и передача ЦТ от НБРК инфраструктурным участникам второго уровня (БВУ/ВУ, госучреждению).

Краткое описание сценариев MVP и R&D

№	Сценарий	Подтвержденные гипотезы	Краткое описание сценария
5	Распределение клиентам (стандартные ЦТ)	<ul style="list-style-type: none"> • Безопасность транзакций • Отслеживаемость 	Процесс передачи ЦТ от БВУ/ВУ конечным пользователям на цифровой кошелек клиента.
6	C2C перевод (по QR)	<ul style="list-style-type: none"> • Сокращение количества посредников • Настраиваемая анонимность • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	Перевод ЦТ от одного физического лица другому на близком расстоянии при помощи передачи реквизитов через QR-код. И устройство отправителя, и устройство получателя подключены к Интернету.
7	C2C перевод (по номеру мобильного телефона)	<ul style="list-style-type: none"> • Сокращение количества посредников • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	Перевод ЦТ от физического лица другому физическому лицу по номеру мобильного телефона. И устройство отправителя, и устройство получателя подключены к Интернету.
8	Маркировка токенов	<ul style="list-style-type: none"> • Сокращение количества посредников • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	Покупка в режиме онлайн с помощью ЦТ через мобильные приложения ТСП и ФЛ (клиенты БВУ/ВУ) с применением QR-кода.
9	Маркировка токенов	Программируемость	Маркировка ГУ (технология «раскрашивания») стандартных ЦТ, распределенных от НБРК
10	Распределение специальных ЦТ клиентам	<ul style="list-style-type: none"> • Сокращение количества посредников • Безопасность транзакций • Отслеживаемость 	Процесс передачи специальных токенов от ГУ конечным пользователям, на цифровой кошелек клиента.

№	Сценарий	Подтвержденные гипотезы	Краткое описание сценария
11	Покупка за специальные ЦТ	<ul style="list-style-type: none"> • Сокращение количества посредников • Программируемость • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	Покупка в режиме онлайн с помощью специальных ЦТ через мобильные приложения ТСП и ФЛ (клиенты БВУ/ВУ) при наличии интернет-соединения с применением QR-кода.
12	Перевыпуск (вкл. техническое погашение)	Непрерывность функционирования	Перевыпуск для снижения нагрузки на производительность. Перевыпуск – это техническое погашение токенов при достижении определенной длины истории транзакций с токеном и выпуск новых токенов без истории.
13	Мониторинг	Отслеживаемость	Бизнес-аналитика и мониторинг нефункциональных параметров
14	Офлайн-платежи (с цепочкой офлайн-транзакций)	<ul style="list-style-type: none"> • Офлайн-транзакции • Непрерывность функционирования 	Цепочка переводов ЦТ с цифрового кошелька на устройстве одного лица на цифровой кошелек другого лица при отсутствии интернет-соединения у обоих участников с использованием QR и NFC (транзакции перевода и покупки).
15	Сценарий внешнего участника (BTS): оплата за проезд	<ul style="list-style-type: none"> • Сокращение количества посредников • Программируемость • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	Покупка в режиме онлайн с помощью специальных ЦТ (оплата за проезд) через мобильное приложение ФЛ при наличии интернет-соединения с применением QR-кода. Имеются ограничения: время использования, сумма использования в сутки, оплата только в определенных ТСП.
16	Сценарии внешнего участника (Евразийский Банк): открытие кошелька, перевод, покупка	<ul style="list-style-type: none"> • Простота интеграции • Сокращение количества посредников • Настраиваемая анонимность • Безопасность транзакций • Непрерывность функционирования • Интероперабельность 	<ul style="list-style-type: none"> • Открытие кошелька ФЛ: первоначальное создание цифровых кошельков для клиентов БВУ/ВУ – физических лиц • С2С перевод (по QR): перевод ЦТ от одного физического лица другому при помощи передачи реквизитов через QR-код • С2С перевод (по номеру мобильного телефона): перевод ЦТ от физического лица другому физическому лицу по номеру мобильного телефона • Оплата покупки в режиме онлайн с помощью стандартных ЦТ • Оплата покупки в режиме онлайн с помощью специальных ЦТ

Функциональные характеристики

Сценарий в рамках проекта – это функциональная характеристика платформы, представляющая собой обобщенное описание действий одного участника или взаимодействия нескольких участников пилотной платформы.

В ходе разработки сценариев учитывались международные и локальные принципы внедрения ЦВЦБ. Сценарии были разработаны таким образом, чтобы:

1. Ориентироваться на покупателя (учитывать интересы покупателя в ходе прохождения по сценариям);

2. Обеспечить равный доступ к системе (относится как к внешним участникам, подключенным к платформе, так и к физическим лицам, осуществляющим транзакции с использованием ЦТ);

3. Повысить интерес рынка к использованию цифровой валюты (путем добавления инновационной функциональности ЦВЦБ: офлайн-платежи, настройка анонимности, программируемость ЦТ).

По каждому из сценариев представлены описания технологических особенностей реализации. Для всех участников – пользователей платформы ЦТ ниже представлен пользовательский путь, в рамках которого пользователи проходят по различным сценариям жизненного цикла ЦТ, а также дополнительным инновационным сценариям. Каждый из шагов в ходе пользовательского пути предоставляет выгоды, новые преимущества и дополнительный функционал для пользователей (Приложение 1).

Результаты пилотирования

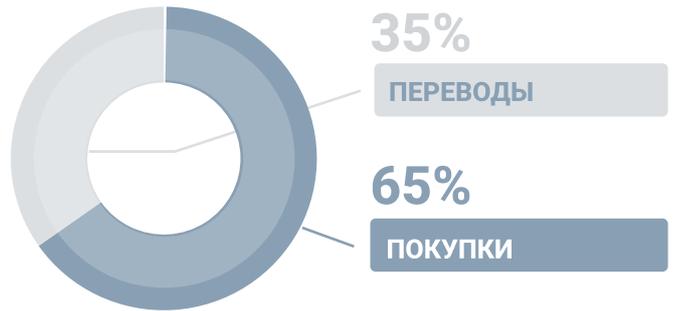
5 
дней

4 
ТСП

200 
пользователей

3 594 
пользователей

ТИПЫ ТРАНЗАКЦИЙ



ТРАНЗАКЦИИ ПО ТИПАМ ЦТ



КОЛИЧЕСТВО ТРАНЗАКЦИЙ В ДИНАМИКЕ



СТРУКТУРА ПЕРЕВОДОВ



РЕЗУЛЬТАТЫ ОПРОСА УЧАСТНИКОВ ПИЛОТИРОВАНИЯ

- 96%** ПОДЧЕРКНУЛИ НЕОБХОДИМОСТЬ ОФЛАЙН-ТРАНЗАКЦИЙ
- 89%** ОЦЕНИЛИ ВАЖНОСТЬ КОНЦЕПЦИИ ПРОГРАММИРУЕМОСТИ ЦТ
- 77%** ОТМЕТИЛИ ВЫСОКУЮ СКОРОСТЬ ТРАНЗАКЦИЙ С ЦТ

Результаты исследования офлайн-платежей (с цепочкой офлайн-транзакций)

Функциональные характеристики

Ключевая цель проекта в рамках анализа офлайн-транзакций – исследование реализуемости цепочки транзакций для каждого пользователя. Разработка данной функциональности повлияет на повышение интереса рынка к использованию цифровой валюты, что соответствует критерию успешности внедрения ЦТ.

На основе исследования зафиксирован ряд результатов:

- технические (защита от двойных трат и противодействие отмыванию доходов (ПОД) и финансированию терроризма (ФТ), применимость и ограничения технологий, требования к устройствам, производительность),
- функциональные (удобство для пользователей, необходимость в пользовательских лимитах).

Для исследования цепочек офлайн-транзакций в R&D зафиксированы следующие **допущения и ограничения**:

Допущения и ограничения исследования цепочек офлайн-транзакций в R&D

Допущения и ограничения

Пользователь может применять режим офлайн на нескольких устройствах, для этого на каждом устройстве открывается отдельный офлайн-кошелек.

В рамках R&D применяется условие: один пользователь = одно устройство. Офлайн- и онлайн-кошелек внутри одного банка.

В рамках R&D и режима демонстрации считается, что пользователи являются благонадежными, не подделывают токены и не совершают нелегальных вмешательств в свои устройства. Проверить происхождение токена в офлайне можно с момента перевода токена на офлайн-кошелек (депозита) на основе подписи БВУ/ВУ (банк выступает гарантом для клиентов).

Офлайн-транзакции реализуются только со стандартными токенами.

Обоснование

Явная привязка офлайн-кошелька (и соответственно ЦТ) к устройству клиента позволяет покрыть один из сценариев двойной траты. Дополнительные устройства для пользователя не соответствуют ключевой цели исследования, но требуют дополнительных трудозатрат.

Обеспечение абсолютной безопасности в офлайн-платежах является сложной и амбициозной задачей, что выходит за рамки текущего исследования. В целевом решении допущение по безопасности предлагается решить на основе решений «последней мили» – программного обеспечения (криптопротоколы; среда безопасного исполнения кода) и/или аппаратных средств (защищенные устройства).

Проведение исследования со специальными токенами не даёт дополнительных выводов, так как основные этапы проведения такой транзакции совпадают со стандартными токенами. Один из этапов проверки при оплате специальными токенами выполняется с мобильного устройства, что не входит в фокус текущего исследования.

Допущения и ограничения исследования цепочек офлайн-транзакций в R&D

Допущения и ограничения

Перевод средств между пользователями происходит **по сценарию перевода (передача реквизитов) и покупки.**

Пользователи используют устройства под ОС Android с характеристиками аналогичными для MVP.

Обоснование

Описание сценария, участников и их функционала для офлайн-транзакции в R&D.

Исследование на Android сохраняет преимущество и переиспользование с этапа PoC. Исследования на двух ОС (Android и iOS) существенно не дополняют исследование, но увеличивают трудозатраты

Для исследования в R&D был составлен список открытых вопросов:

- возможные механизмы снижения риска двойных трат, отмывания денег и финансирования терроризма
- возможные технологии для проведения цепочки транзакций в офлайне на основе удобства для пользователей
- возможная длина цепочки офлайн-транзакций
- технические требования и ограничения к устройствам пользователей для проведения офлайн-транзакций
- анализ необходимости введения функциональных лимитов, применяемых к отдельному офлайн-кошельку
- влияние офлайн-транзакций на производительность нод

Результаты по итогам проведенного исследования представлены в Приложении 1.

Исследование офлайн-платежей в других странах

Ниже представлены примеры подходов к офлайн-платежам в разных странах

Примеры подходов к офлайн-платежам

Страна

Подход

Казахстан

В 2022 году протестирована цепочка офлайн-транзакций с предварительной передачей на устройство клиента информации о ЦТ, заверенной банковской подписью.

Россия [7]

Для совершения офлайн-операций помимо онлайн-кошелька клиенту открывается второй кошелек в цифровых рублях на мобильном устройстве. Пополнение офлайн-кошелька осуществляется клиентом путем перевода цифровых рублей с онлайн-кошелька (при наличии доступа к сети Интернет).

Страна	Подход
Швеция [5]	В рамках второй фазы проекта по разработке E-krona в 2021 году проводилось тестирование офлайн-сценариев: хранение токенов и ключей производилось локально на мобильном устройстве, для передачи данных использовалась технология NFC. Для синхронизации транзакций требовалось подключение к Интернету одного из участников транзакции.
Китай [4]	В сотрудничестве с производителями мобильных телефонов Народный банк Китая исследует офлайн-платежи с использованием смарт-карт.
Южная Корея [6]	Банк Кореи планирует к запуску офлайн-тесты в рамках проекта ЦВЦБ на смартфонах, умных часах и планшетах Galaxy от Samsung Electronics Co.

Результаты исследования перевыпуска токенов (включая техническое погашение)

Перевыпуск – замена старого токена с длинной цепочкой транзакций на новый без истории. Сценарий предназначен для оптимизации производительности: поскольку с ростом истории увеличивается время процессинга транзакции, необходимо ограничить максимальную длину истории транзакций для токена, чтобы соответствовать требованиям по максимальной длительности проведения транзакции.

В рамках направления MVP проведено исследование сценария перевыпуска токенов.

Ключевыми целями данного исследования являются:

- оптимизация производительности платформы и времени проведения транзакции за счет сокращения истории токена и времени ее проверки;
- повышение уровня анонимности платформы ЦТ за счет усложнения отслеживаемости разорванных цепочек транзакций

В рамках сценария было выбрано значение «накопления» счётчика в истории токена для проведения перевыпуска, с учетом следующих факторов:

- оптимизация длительности проведения транзакции клиентов;
- возможные маршруты транзакций клиентов в рамках пилота;
- оптимизация нагрузки на систему от транзакций перевыпуска.

В ходе исследования зафиксированы риски перевыпуска и предложены способы работы с ними. Отсутствует атомарность перевыпуска (перевыпуск состоит из нескольких операций), ответственность лежит на разных участниках (нет единого актора, принимающего участие в каждой из транзакций), нет единого контракта (транзакция является валидной, если все контракты в ней исполнились без ошибок, но контракты находятся внутри транзакций и не связывают их). Технически все четыре транзакции нельзя объединить в одну.

Для работы с рисками потери клиентом денежных средств в процессе перевыпуска используются следующие механизмы:

- последовательность транзакций: сначала новые токены зачисляются клиенту, а затем старые отправляются в НБРК;

- осуществлены проверки, не позволяющие БВУ/ВУ потратить эмитированный в рамках перевыпуска токен вне перевыпуска;
- при отправке запроса в НБРК, БВУ/ВУ отмечает перевыпускаемый токен как находящийся в процессе перевыпуска. Как только токен отмечен таким образом, его нельзя потратить, поскольку для него начался процесс перевыпуска.

Нефункциональные характеристики

Производительность

В рамках пилотного проекта проводилось тестирование производительности для подготовки к проведению проекта, а также проверка системы на возможность обеспечивать необходимый уровень производительности с реальными пользователями. В ряде тестов ключевыми областями исследования были:

- скорость проведения транзакций (секунды)
- ошибки при проведении транзакций (проценты)
- эффект от увеличения параметров инфраструктуры
- замер использования ресурсов (CPU, RAM)
- потенциальные области оптимизации

Разработанная платформа ЦТ может работать как на базе Corda Community Edition (CCE), так и на базе Corda Enterprise Edition (CEE). На основе результатов и исследований нагрузочного тестирования выявлено, что платформа покрывает требования к пропускной способности пилотного проекта. Но для достижения показателей в условиях промышленного масштаба необходимо реализовать ряд дополнительных задач по оптимизации производительности при разработке решения, как на базе CCE, так и CEE.

Наибольшее влияние на производительность решения оказывают:

- наличие стандартных процессов Corda по резервному копированию, на которые приходится свыше 75% данных при обработке каждой транзакции;
- наличие/отсутствие многопоточной обработки транзакций;
- однопоточная обработка при проверке истории транзакций токена.

Дальнейшие рекомендации по оптимизации описаны в Приложении 1.

Результаты производительности в пилотном проекте

В рамках пилотного проекта удалось поддержать комфортный для пользователей уровень производительности для совершения транзакций за счет организационных мер (организация маршрутов транзакций пользователей в рамках пилотного проекта, ограничение количества пользовательских транзакций), механизма перевыпуска токенов, а также за счет повышения устойчивости системы к нагрузке.

Результаты пилотного проекта доказали технологическую реализуемость сценариев жизненного цикла и возможность применения инновационных свойств ЦТ. Оптимизация производительности не являлась фокусным направлением в рамках пилотного проекта. В рамках нагрузочного тестирования разработанной платформы ЦТ были проведены замеры пропускной способности и времени ответа, в том числе с применением

методов оптимизации и настройки конфигураций, время на полноценное тестирование производительности и стабильности платформы, тонкую настройку на данном этапе не было заложено.

Результаты пилотного проекта показали, что производительность платформы на уровне показателей платежных систем является одним из ключевых вызовов на будущее. Платформа ЦТ на следующем этапе потребует глубокой проработки вопросов производительности и выделения отдельной фазы для исследования, оптимизации и достижения целевых показателей платформы: повышения пропускной способности, сокращения длительности обработки транзакции, решения вопроса увеличения длительности обработки транзакции при увеличении истории (помимо перевыпуска токенов) и т.п.

Наблюдаемость и мониторинг

Предусмотрена **возможность логирования** (отслеживание статуса работы системы и ее компонентов), а также **технического мониторинга** инфраструктуры MVP пилотной платформы, **мониторинг нефункциональных показателей и подготовка данных для бизнес-статистики**.

Интероперабельность

В контексте ЦВЦБ интероперабельность является сложным предметом для рассмотрения из-за большого количества взаимодействий и различий в формате данных с форматами, определенными в существующих стандартах. В рамках пилотного проекта была осуществлена **проверка интероперабельности в двух аспектах**: совместимость с международными стандартами в части передачи финансовых сообщений и совместимость с международными стандартами и национальными стандартами Казахстана в части QR-кодов.

Для проверки **совместимости платформы ЦТ с международными стандартами передачи финансовых сообщений** формирование спецификаций API и разработка API пилотной платформы ЦТ происходило с учетом потенциальной применимости платежных стандартов ISO 20022 [2]. Полная совместимость не была достигнута, поскольку существующими стандартами не поддерживаются форматы платежных сообщений для транзакций с токенизированными ЦВЦБ, реализуемыми с применением криптографических механизмов, предполагающими передачу публичных адресов, подписей. При этом расхождения в передаваемых параметрах увеличиваются при добавлении функций по анонимности и программируемости.

Для проверки **совместимости платформы ЦТ с международными стандартами и национальными стандартами Казахстана в части QR-кодов** разработка требований к QR-кодам производилась с учетом существующего национального стандарта СТ РК 3712-2021 [9] (требования к составу данных QR-кода для приема платежей), а также международного стандарта ISO 18004 (спецификация символики QR-кода) [3].

При разработке требований к QR-кодам использовалась модификация существующего стандарта СТ РК 3712-2021 [9] (требования к

составу данных QR-кода для приема платежей) с возможностью проведения переводов и платежей в цифровой валюте.

Таким образом, совместимость с международными стандартами в части передачи финансовых сообщений пока нереализуема из-за уникальных особенностей данных, передаваемых на платформе ЦВЦБ. Полная совместимость с международными стандартами и национальными стандартами Казахстана в части QR-кодов также требует модификаций существующих стандартов.

Аспекты информационной безопасности

В качестве ключевых аспектов, характеризующих уровень защищенности платформы ЦТ и на основе модели угроз, а также нарушителя, был определен ряд направлений информационной безопасности. В рамках каждого аспекта сформирован набор требований по информационной безопасности и проведена оценка платформы ЦТ на соответствие этим требованиям.

Управление доступом

Процесс управления доступом реализован с учетом персонификации всех действий, совершаемых от имени пользователей, а также процессов, запускаемых от имени системных учетных записей. При этом использовался **принцип группирования пользователей**. Реализация методов ролевой модели при разграничении логического доступа позволяет **оптимально решать проблемы инвентаризации** существующих прав доступа учетных записей. Парольные политики, применяемые в системе, в полной мере соответствуют лучшим практикам информационной безопасности.

Управление журналами аудита

Журналы событий содержат достаточный набор данных для потенциального расследования инцидентов нарушения безопасности (учтена такая информация как идентификаторы пользователей, время начала и завершения сеанса, информация о выполняемой операции, успешные и отклоненные попытки доступа к системе). Факт наличия конфиденциальной или избыточной информации не зафиксирован.

Инвентаризация и учет

В целях корректности процедур и процессов управления журналами аудита осуществляется синхронизация системного времени компьютера через сетевое соединение. Данный контроль обеспечивает согласованную работу продукта и позволяет эффективно и своевременно расследовать внутренние инциденты и контролировать возможные нарушения безопасности.

Управление инцидентами ИБ

Процесс управления инцидентами предполагает формализованный шаблон для регистрации инцидентов с указанием основных параметров инцидента для определения задействованных функциональных единиц платформы ЦТ. Для выявляемых инцидентов введена трехуровневая классификация по критичности, зафиксированы нормативные сроки оповещения ответственных лиц и проведения расследования.

Конфигурация устройств и ПО

Архитектура сред платформы ЦТ реализована таким образом, что продуктивная среда отделена от тестовой и среды разработки для снижения рисков внесения неавторизованных изменений в продуктивную среду и, как следствие, потери доступности платформы и/или целостности данных.

Криптографические механизмы защиты информации

Для обеспечения безопасности передаваемой информации с точки зрения конфиденциальности и целостности в соответствии с лучшими практиками применяются алгоритмы шифрования с использованием протоколов TLS и SSH. Хранимые пароли доступа к базе данных защищены с помощью алгоритма шифрования SHA-512. Применяются асимметричные алгоритмы криптографии (криптография на эллиптических кривых): алгоритмы подписи и проверки подписи, создания одноразовых stealth-адресов и одноразовых частных ключей к ним, скрывание сумм с помощью обязательства Педерсена.

Безопасность разработки и управление уязвимостями

Для работы на платформе используются только проверенные модули шифрования, ведения журналов, управления идентификацией пользователей, а также зависимости.

В связи с тем, что целевая платформа является критически важной для жителей РК, необходимо реализовать усиленные меры защиты, способные сохранить денежные средства, а также финансовую стабильность РК. Для этого в целевой платформе необходимо:

- обеспечить разработку платформы с учетом всех необходимых технических средств, принципов и практик в области ИБ;
- реализовать сетевую защиту платформы и каналов связи;
- обеспечить управление доступом и правами к платформе;
- реализовать антивирусную защиту информации;
- осуществить мониторинг, обнаружение и реагирование на инциденты ИБ;
- обеспечить управление привилегированным доступом, а также доступом подрядчиков;
- реализовать защиту данных от утечек;
- внедрить иные меры на основе рисков и лучших практик в сфере ИБ.

Выводы и оценки

Оценка технологического эффекта

В рамках проекта были достигнуты следующие результаты:

1. Возможности программирования. В MVP реализована и протестирована программируемость ЦТ совместно с внешними участниками, а именно возможность задания ограничений использования ЦТ в структуре токена для упрощения отслеживаемости целевого использования ЦТ. В дальнейшем функционал и возможности программирования ЦТ будут расширены (например, реализация смарт-контрактов). Технологическая реализуемость данного функционала – **значение С (данный аспект на данный момент технологически реализуем, но его реализация может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).**

2. Гибкость системы. В проекте оценивалась потенциальная применимость платежных стандартов ISO 20022 [2], а также реализована интеграция с мобильными приложениями, разрабатываемыми внешними участниками (банками второго уровня, финтех-компаниями). В дальнейшей реализации проекта необходима интеграция с продуктивными приложениями и системами (НБРК, ГО, БВУ/ВУ, ТСП), интеграция с платежными системами и национальными сервисами. Технологическая реализуемость данного функционала – **значение С (данный аспект технологически реализуем, но его реализация может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).**

3. На основе проведенного тестирования в R&D доказана технологическая реализуемость возможности проведения **транзакций в офлайне, включая цепочку офлайн-транзакций.** Для реализации офлайн-платежей в промышленном решении требуется доработка текущего решения (использование нескольких устройств в офлайне и др.), детальная проработка «последней мили», проработка регуляторных вопросов, возможности восстановления, что требует существенных ресурсов и исследовательской работы (совместно с вендорами решений). На основании модели принятия решения [8] данной категории технологического эффекта присвоено **значение D (данный аспект технологически реализуем, но его реализация может потребовать отдельного фундаментального исследования и/или среднего объема ресурсов).**

ТЕХНОЛОГИЧЕСКИЙ ЭФФЕКТ



Итоговая оценка по технологическому эффекту – значение С (данный аспект технологически реализуем, но его реализация может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).

Оценка технологических рисков и киберрисков

В ходе реализации проекта были выявлены следующие технологические риски:

1. На текущий момент на рынке **нет технологических решений, полностью удовлетворяющих требованиям и свойствам ЦТ**, на основе которых реализована ЦВЦБ какой-либо страны в продуктивной или пилотной стадии. Отсутствие подтвержденной технологии распределенных реестров и технологической архитектуры ставит под риск реализацию пилотного внедрения в сжатые сроки, а также не дает возможность в полной мере оценить объем работ, сроки, ресурсы и стоимость проекта.

2. Выбор платформенного решения от вендора позволяет уменьшить неопределенность в сроках разработки, но ограничивает ЦВЦБ функционалом «из коробки», а также создает сильную зависимость от лицензии на использование, доработок функционала на стороне вендора и доступности команды поддержки для обеспечения надежности решения. При выборе целевой платформы следует рассматривать те технологии (и вендоров, поддерживающих разработку), которые позволят обеспечить **национальный технологический суверенитет Казахстана**.

3. **Риск зависимости от технологической зрелости внешних участников** – качественная реализация продукта возможна при тесном взаимодействии с внешними участниками. Для реализации целевой платформы от внешних участников потребуются существенные инвестиции в развитие решений (определенный уровень технологического стека и безопасности мобильных приложений, наличие компетенций и инфраструктуры для интеграции с платформой ЦТ, возможность функционального развития на базе ЦТ и совместимость с основным бизнесом внешнего участника).

4. **Риски производительности и стабильность решения.** В силу незрелости технологии, незначительного количества промышленных внедрений, существует риск того, что платформа не позволит обеспечить производительность, сопоставимую с существующими решениями национального уровня, например, с карточными системами. На текущий момент в закрытых тестовых окружениях Corda и другие технологические платформы демонстрируют допустимые результаты по производительности, сопоставимые с существующими системами (например, системы быстрых платежей), но их приемлемость для продуктивного решения должна тестироваться в условиях, приближенных к реальным.

5. **Безопасность решения** в целом обеспечивается с двух сторон: встроенные контроли на уровне платформы, а также безопасность на уровне пользователя.

a. **Безопасность на уровне платформы.** На данный момент отсутствуют рекомендации относительно наиболее безопасной реализации защиты на уровне платформы, в качестве альтернатив предлагаются алгоритмическая криптозащита, безопасность на основе аппаратного или программного обеспечения или их комбинация. Каждый вариант несет определенные риски с точки зрения достигаемого уровня защиты, сложности реализации и поддержки в виду «гонки вооружений» между атаками и защитой.

b. **Безопасность на уровне пользователя (безопасность решений «последней мили»).** Безопасность на уровне пользователя должна гарантироваться выбранным решением «последней мили» (мобильное приложение, смарт-карты и т.п.). Пока такие решения не приняты, но в ходе аналитического исследования были выявлены потенциальные решения, требуются взаимодействия с поставщиками и партнерами для дальнейшей проработки.

Для оценки технологических рисков была использована шкала оценки от А до F в соответствии с Моделью принятия решений по следующим критериям:

- уровень влияния рисков (где А – риски незначительны, F – внедрение ЦТ связано с существенными технологическими рисками);
- возможность митигации (где А – митигация возможна, F – митигация невозможна);
- стоимость митигации (где А – митигация не потребует дополнительных ресурсов, F – митигация потребует значительных дополнительных ресурсов).

Каждый вышеупомянутый риск оценивался по трем критериям. Основываясь на перечисленных выше рисках, можно сделать вывод, что риски существуют, но они могут быть митигированы. Таким образом, оценка по технологическим рискам внедрения ЦТ – «С» (митигация технологических рисков данного подхода может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).

ТЕХНОЛОГИЧЕСКИЕ РИСКИ



Киберриски

В ходе формирования частной модели угроз информационной безопасности идентифицированы наиболее актуальные угрозы безопасности и их источники, предпосылки к их реализации и вероятные объекты атак.

Последствия в случае реализации угроз определяются с помощью анализа возможного негативного эффекта при воздействии на три составляющих аспекта информационной безопасности: конфиденциальность (К), целостность (Ц), доступность (Д) информации, обрабатываемой платформой. Оценка производится в ходе обсуждения возможных негативных сценариев развития событий, из которых выбираются наиболее существенные по каждому из направлений КЦД.

По результатам анализа модели угроз наиболее уязвимыми объектами

платформы были выделены Узел (Node), Базы данных узла (Node) и сетевая инфраструктура. В случае компрометации сетевой инфраструктуры или при наличии скомпрометированных узлов, на которых запущены приложения CorDapp с вредоносным кодом, возможна реализация ряда угроз, зачастую имеющих негативное влияние на конфиденциальность обрабатываемой информации, а также доступность платформы. Для предотвращения возможных угроз и снижения вероятности их реализации рекомендован список базовых и продвинутых контролей с фокусом на проактивное управление корпоративными активами, подключенными к инфраструктуре физически, виртуально, удаленно, а также с помощью облачных технологий.

По итогам проведенного анализа уровня защищенности информации, обрабатываемой

в рамках платформы ЦТ, был выявлен ряд несоответствий требованиям информационной безопасности. Большая часть несоответствий касается низкого уровня формализации процессов обеспечения информационной безопасности в виде политик и прочих регламентирующих документов. Важно понимать, что на текущем этапе разработки (MVP) платформы **не предполагается обеспечение доступа пользователей к данным продуктивной среды.**

В рамках проекта обеспечивается как минимум **базовый уровень защищенности**, за счет чего **значительно снижается потенциальный риск реализации инцидентов ИБ** и ущерба конфиденциальности, целостности и доступности платформы и

соответствующих данных. Для повышения уровня защищенности необходимо проведение работ по определению набора средств информационной безопасности, планированию их поэтапного внедрения и поддержки.

По результатам проведенного анализа уровень защищенности платформы соответствует оценке С (митигация технологических рисков данного подхода может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).

КИБЕРРИСКИ



Итоговая оценка по технологическим рискам и киберрискам – значение С (митигация технологических рисков данного подхода может потребовать отдельного дополнительного исследования и/или малого объема ресурсов).

Выводы и оценки

Результаты проекта подтвердили технологическую реализуемость требований, предъявляемых к ЦТ

Результаты проекта подтвердили технологическую реализуемость требований, предъявляемых к ЦТ. Технологический эффект реализуем, но его реализация может потребовать отдельного дополнительного исследования и/или малого объема ресурсов.

Митигация технологических рисков может потребовать отдельного дополнительного исследования

Митигация технологических рисков может потребовать отдельного дополнительного исследования и/или малого объема ресурсов.

Промышленное решение платформы ЦТ предполагает расширение базовых сценариев для создания конкурентного средства оплаты, используемого всем населением страны

Промышленное решение платформы ЦТ предполагает расширение базовых сценариев для создания конкурентного средства оплаты, используемого всем населением страны. В качестве рекомендаций для проработки в рамках продуктивного решения стоит выделить ряд новых функций по следующим направлениям:

- создание инфраструктуры для разработки сложных сценариев использования ЦТ;
- создание целевой API management платформы для упрощения интеграции и управления доступом к платформе ЦТ;
- внедрение процессов и инструментов для интеграции разработок внешних участников в платформу ЦТ;
- разработка компонентов для получения и валидации внешних данных на уровне платформы ЦТ, в том числе для разработки смарт-контрактов;
- выбор last mile решения с фокусом на безопасную реализацию платежей на уровне страны;
- оптимизация производительности платформы ЦТ для высокой нагрузки;
- включение платформы ЦТ в национальный и международный финансовый ландшафт;
- интеграция с базовыми универсальными сервисами национального уровня;
- интеграция с национальными и международными системами;
- интеграция с другими DLT-системами.

ЭКОНОМИКА

51-58

стр.

Дизайн ЦТ

ЦТ будет дополнять существующие платежные системы и не должен влиять на финансовую и макроэкономическую стабильности

Экономический дизайн ЦТ основывается на международных принципах внедрения ЦВЦБ. ЦТ будет дополнять существующие платежные системы и не должен влиять на финансовую и макроэкономическую стабильности. В связи с этим в дизайне ЦТ не рассматривается начисление процентов, ЦТ в первую очередь позиционируется как инструмент платежа. Сохраняется двухуровневая цифровая платежная система с участием НБРК и провайдеров платежных услуг.

Риск перетоков ликвидности из банковского сектора в обязательства НБРК может быть митигирован за счет лимитов и других мер финансового регулирования

Оценка экономических эффектов при внедрении ЦТ в 2021 году показала, что при его эмиссии не произойдет увеличения денежной базы и денежной массы в экономике, будут наблюдаться лишь изменения структуры в денежном предложении. Также потенциальный риск перетоков ликвидности из банковского сектора в обязательства НБРК может быть митигирован за счет лимитов – допустимых объемов конвертации текущих счетов в ЦТ и других мер финансового регулирования. Согласно последним исследованиям БМР, предлагаемые меры для устранения рисков перетока средств в ЦВЦБ группируются на две категории: количественные и ценовые меры (Приложение 2).

В рамках модели принятия решений в 2022 году проведен количественный анализ для оценки двух критериев: экономических эффектов и рисков.

Гипотезы и вопросы исследования

Экономический эффект

Внедрение ЦТ потенциально принесет целый ряд совершенно новых цифровых возможностей и преимуществ для всех граждан: потребителей, финансовых организаций и государственных институтов.

Вопросы исследования:

1. Каким будет спрос на ЦТ?
2. Какие из атрибутов (характеристик) дизайна ЦТ – стоимость использования, простота/удобство использования, безопасность, анонимность, полезность для составления бюджета и др. – повлияют на спрос?
3. В какой степени ЦТ повлияет на спрос на наличные деньги и средства на текущих счетах?

Экономические риски

Наряду с потенциальными выгодами существуют экономические риски от внедрения ЦТ: изменение макроэкономических параметров, влияние на финансовую стабильность.

Вопросы исследования:

1. Как будут изменяться макроэкономические переменные при разных свойствах ЦТ?
2. Как различные правила внедрения ЦТ влияют на банковское кредитование и деятельность по займам в экономике?
3. Какое будет влияние ЦТ на ДКП?

Подход к оценке

В экономике для получения количественных ответов применяются инструменты моделирования, которые строятся на основе эмпирических данных. В случае прогнозирования спроса на ЦТ, как и на другие ЦВЦБ, необходимо учитывать отсутствие реальных данных по использованию платежных инструментов.

Согласно международной практике, для оценки спроса на ЦТ необходимо оценить поведение и отношение пользователей к существующим платежным инструментам и к сектору банковских услуг. В этих целях в большинстве случаев используются количественные методы оценки на основе интернет-опросов населения (Приложение 2).

Опрос

В Казахстане разработана методология проведения опросов с учетом дизайна ЦТ, социально-экономических показателей граждан РК, специфики финансового рынка, характеристик различных видов продуктов (наличные деньги, депозиты, кредитные карты и т.д.).

В отличие от других опросов в данный опрос ЦВЦБ были включены не только вопросы о действующих платежных инструментах в Казахстане, но также о характеристиках,

которые пользователи хотели бы видеть у ЦТ. Кроме того, предлагались вопросы для определения готовности казахстанцев принять ЦТ, чтобы понять, какие характеристики наиболее важны для различных слоев населения. Эти вопросы также являются прямыми индикаторами настроения населения, уровня доверия и спроса на ЦТ. Чтобы понять, как меняется отношение респондентов до и после получения информации, вопросы анкеты о ЦТ дублировались после краткого объяснения респондентам о ЦТ.

Был проведен онлайн-опрос (CAWI – Computer Assisted Web Interviewing) среди 3000 респондентов. В целях репрезентативности выборки предусматривалось квотирование количества респондентов по всем регионам РК с учетом демографической статистики, то есть пропорционально доле взрослого населения в регионе к общей численности взрослого населения. Данные опроса использовались для построения микромоделей оценки эластичности замещения ЦТ и определения потенциального спроса на ЦТ.

Эконометрическая модель

Потенциальный спрос на ЦТ прогнозировался на основе эконометрической модели, были выявлены соответствующие характеристики ЦТ и домохозяйств, которые влияют на спрос на ЦТ (Приложение 2).

Проводилась оценка постоянной эластичности замещения между ЦТ и денежными средствами, то есть насколько легка или сложна взаимозаменяемость между наличными и ЦТ. Чем выше эластичность, тем выше их взаимозаменяемость.

Успех внедрения ЦТ зависит от понимания того, какие качества платежных инструментов являются наиболее важными с точки зрения потребителей, а также факторов, повышающих вероятность использования ЦТ. Чтобы изучить отношение потребителей к внедрению ЦТ, построена модель, которая оценивает влияние различных социально-демографических

факторов, знание ЦТ, осведомленность о криптовалютах, важность различных характеристик ЦТ, удобство использования наличных и анонимность, доверие к обслуживающему банку и НБРК. Кроме того, анализируются потребители, которые часто используют наличные и мобильные приложения для совершения платежей.

Особенностью методологии исследования является возможность изучения влияния различных факторов, состоящих из комбинаций переменных Abramova et al. (2022), Bijlsma et al. (2021) и других важных факторов, благодаря опросным данным, включающим широкий спектр вопросов.

Была рассчитана вероятность принятия ЦТ гражданами РК. На ее основе произведена оценка влияния ЦТ на макроэкономические параметры и финансовую стабильность, а также благосостояние населения.

2 DSGE модели

Оценка постоянной эластичности замещения ЦТ была внедрена в две DSGE модели (среднемасштабная модель динамического стохастического общего равновесия).

Модели учитывают не только уникальную структуру экономики Казахстана через уравнения, но также учитывают специфическое восприятие домохозяйствами ЦТ и других форм денежных средств в Казахстане.

Уникальность подхода для Казахстане основана на использовании оценочного параметра полученных опросных данных: эластичности спроса на ЦТ, так как в других странах используют косвенные параметры из-за отсутствия опросных данных и возможности оценки эластичности спроса на ЦВЦБ напрямую. Исследования фиксируют коэффициент эластичности замещения на значениях, не подкрепленными эмпирическими оценками. Также макро- и микроисследования проводятся разными исследователями, что не позволяет оценивать данный параметр в микромодели. (Приложение 2).

Эластичность спроса на ЦТ: на сколько процентных пунктов меняется соотношение ЦТ и денежных средств на изменение в один процентный пункт в относительных издержках ЦТ и денежных средств. Издержки – стоимость хранения, комиссии использования, цена – процентная ставка на ЦТ.

В целом существует лишь ограниченное количество работ, анализирующих наличие ЦВЦБ в модели DSGE. Основные выводы



01

Опрос

Проведен опрос 3000 потребителей по всем регионам РК для сбора данных



02

Промежуточная модель

Далее на основе данных проведен микроэконометрический анализ - оценен спрос на ЦТ



03

Две DSGE-модели

Результаты были интегрированы в 2 DSGE-модели для оценки влияния ЦТ на макропараметры, финансовую стабильность, благосостояние населения РК

Результаты исследования

Каким будет спрос на ЦТ?

Около 60% опрошенных выразили готовность использовать ЦТ. Наиболее важные для респондентов характеристики ЦТ – повсеместность приема к оплате, безопасность (защита от мошенничества и краж) и отсутствие комиссий за использование.

Мужчины в сравнении с женщинами оказались более заинтересованы в использовании ЦТ, респонденты более состоятельных семей наиболее склонны попробовать новый инструмент платежа, респонденты более старшего возраста менее заинтересованы в ЦТ. Люди старше 50 лет менее готовы использовать ЦТ, но разница с категорией до 50 лет невелика – около 54% изъявили желание использовать ЦТ.

В опроснике вопрос о готовности использовать ЦТ был задан дважды, чтобы увидеть, как более высокая осведомленность о ЦТ отражается на склонности к использованию: до и после прочтения информационной заметки с описанием основных характеристик ЦТ.

Действительно, заинтересованность респондентов в использовании ЦТ оказалась сильнее при повышении осведомленности по этой теме.

В оценке спроса на ЦТ применялся сценарный анализ, так как в зависимости от различного дизайна ЦТ желание его использовать может меняться. Чаще люди исходят из существующей практики при оценке полезности ЦТ.

Какие атрибуты (характеристики) дизайна ЦТ, такие как стоимость использования, простота/удобство использования, безопасность, анонимность, полезность для составления бюджета и др., повлияют на спрос?

Были проанализированы пять сценариев: когда ЦТ имеет базовый дизайн, дизайн как у наличных, депозита, карты, мобильного

приложения. Дизайн в сценариях определялся следующими характеристиками ЦТ: удобство, стоимость, безопасность, анонимность, повсеместное принятие, удобство для ведения личных финансов (usefulness for budgeting), банковская комплектация (bank bundling) – индикатор доверия к банкам и лояльности.

Однако есть и вторая сторона дизайна. Важно не только как он спроектирован со стороны провайдера платежных услуг, но и как его воспринимает и использует сам потребитель. Например, возможно открыть депозит, но ежедневно использовать его как текущие средства и воспринимать как наличные средства.

В рамках базового сценария делается допущение, что ЦТ более схож с наличными деньгами: не связан с банковскими услугами, беспроцентный, широко и повсеместно используется, имеет такой же уровень удобства, стоимости использования и безопасности, что и наличные. Также допускается, что ЦТ может достигать 70% анонимности денежных средств и полезности при составлении бюджета. Таким образом при базовом сценарии и дизайне как у наличных спрос на ЦТ практически одинаковый.

При базовом сценарии прогнозируемый спрос на ЦТ за месяц колеблется от 9,7% до 24,4% доступных средств на использование, в зависимости от того, как человек воспринимает ЦТ: ближе к наличности или банковским депозитам.

Если потребитель будет использовать ЦТ как инструмент оплаты, тогда на аналоги наличных средств спрос составит 9,6%. Если человек будет использовать ЦТ в виде карты, тогда спрос составит 38,4%. В сценарии хранения средств в банке в качестве депозита спрос составит 48,1%.

Восприятие пользователя ЦТ

Дизайн ЦТ со стороны провайдера услуг	воспринимает как наличные	воспринимает как депозит
Базовый дизайн	9,7%	24,4%
Дизайн как у наличных	9,6%	24,1%
Дизайн как у депозита	23,8%	48,1%
	воспринимает как наличные	воспринимает как банковскую карту/ приложение
Дизайн как у карты	24,5%	38,4%
Дизайн как у мобильного приложения	19,5%	26,5%

Однако в дизайне ЦТ, аналогичному мобильному платежному приложению, спрос на ЦТ снизится до 26,5%. Одна из главных причин заключается в том, что в настоящий момент люди воспринимают более высокую полезность от использования мобильных платежей. Переход с мобильных платежей на ЦТ может быть сложнее, чем с платежей наличными или картой на ЦТ.

Таким образом, уровень проникновения ЦТ во многом зависит от дизайна ЦТ, который должен включать в себя функции мобильных платежных приложений.

Уровень проникновения ЦТ зависит от понимания того, какие качества платежных инструментов являются наиболее важными с точки зрения потребителей, а также факторов, повышающих вероятность использования ЦТ.

Прогнозируемая вероятность населения принять ЦТ составляет 66,5%. Вероятность использовать ЦТ увеличивается благодаря высокой скорости расчета, удобству и использованию посредством смартфонов.

Люди с более высоким уровнем дохода имеют высокую вероятность принятия ЦТ, то же самое касается их статуса занятости. Наемные работники и самозанятые имеют более высокую прогнозируемую вероятность принятия ЦТ в сравнении с безработными. Люди, владеющие бизнесом, имеют вероятность принятия ЦТ в 58,3% (наименьшую среди всех групп занятости). Это означает, что бизнес менее заинтересован и более осторожен в принятии ЦТ.

При это понимание отношения бизнеса к ЦТ является еще одним решающим фактором успешного внедрения ЦТ, который важно изучить в будущих исследованиях.

В какой степени ЦТ повлияет на спрос на наличные деньги и средства на текущих счетах?

Эластичность замещения между наличными деньгами и ЦТ равна 0,735. Это означает, что обычный пользователь не готов на 100% заменить наличные средства на ЦТ. Например, если ЦТ по отношению к наличным деньгам менее анонимен, менее удобен с точки зрения ведения личных финансов, ЦТ не сможет полностью заменить наличные. При этом коэффициент демонстрирует высокий уровень взаимозаменяемости.

Эластичность замещения между текущими счетами и ЦТ составляет 0,609. Пользователи менее готовы заменить средства на текущих счетах на ЦТ в сравнении с наличными. Удобства от использования средств на текущих счетах определяют степень перетока безналичных средств на ЦТ. Текущий анализ показывает, что потребители не воспринимают ЦТ как 100% замену безналичных средств.

Как будут изменяться макроэкономические переменные при разных свойствах ЦТ?

Сценарный анализ по макроэкономической стабильности

Были проанализированы различные сценарии:

1. ЦТ с нулевой процентной ставкой
2. Выпуск ЦТ как 10% от ВВП
3. ЦТ с фиксированной ставкой в 2%
4. ЦТ с варьируемой ставкой, когда процентная ставка определяется через правило Тейлора

С точки зрения макроэкономической стабильности наиболее оптимальным является сценарий с нулевой процентной ставкой, так как он оказывает наименьшее влияние на объем производства, уровень инфляции, обменный курс и дефицит бюджета.

В случае нулевой процентной ставки по ЦТ объем ЦТ в долгосрочной перспективе составит от 5,7% до 6,2% ВВП. Другими словами, согласно экономическому понятию долгосрочного устойчивого состояния экономики при нулевой процентной ставке по ЦТ население будет готово держать ЦТ в объеме от 5,7% до 6,2% от ВВП.

В данном случае отсутствует риск для финансовых институтов – при оттоке текущих счетов физических лиц из БВУ в ЦТ доходность банковского сектора не изменится, так как ЦТ не является альтернативой для депозитов и не влияет на кредитование в экономике.

Как различные правила внедрения ЦТ влияют на банковское кредитование и деятельность по займам в экономике?

Для изучения роли ЦТ в сфере финансовой стабильности в Казахстане построена DSGE-модель с номинальной и реальной жесткостью, включающая банковский сектор, который характеризуется монополистической конкуренцией. Модель основана на работе Gerali et al. (2010), в которой изучается роль финансовых трений и банковского

посредничества в деловых циклах. Модель дополнена предпочтениями ликвидности в функции полезности домохозяйств, которая состоит из наличных средств и ЦТ. Далее модель оценивается с помощью байесовских методов, используя макроэкономические и финансовые данные по Казахстану, затем оцениваются показатели структурных параметров. Экономика населена континуумом вкладчиков, заемщиков и предпринимателей. Выбраны следующие переменные для определения финансовой стабильности: процентный спред банков (разница между ставками по кредитам и депозитам), отношение собственного капитала банков к активам, рентабельность активов и рентабельность собственного капитала банков.

При нулевой процентной ставке ЦТ используется в экономике как платежное средство, и оптимальный объем спроса на ЦТ домохозяйствами составляет от 5,7% до 6,2% от ВВП. В данном сценарии внедрение ЦТ незначительно влияет на прибыль БВУ и показывает, что прибыль БВУ растет на 0,1% в устойчивом состоянии (незначительное изменение). Внедрение ЦТ влияет на структуру наличных средств и средств на текущих счетах населения, которые не являются источником фондирования для выдачи кредитов. С этой точки зрения ЦТ не оказывает влияния на процесс формирования прибыли и капитал БВУ (Приложение 2).

При этом для прогнозирования новых доходов от внедрения инновационных сценариев с ЦТ должны быть проведены дальнейшие опросы представителей бизнес-сектора в следующем году.

Каким будет влияние ЦТ на денежно-кредитную политику?

Механизмы передачи финансовых шоков практически неизменны из-за близкой взаимозаменяемости наличных средств и ЦТ. Импульсные отклики ключевых макроэкономических переменных в базовом сценарии без ЦТ и в сценариях с ЦТ отличаются только величиной, но не направлением импульсных откликов.

Внедрение ЦТ позволяет НБРК влиять на экономические процессы посредством выпуска и изъятия ЦТ из обращения. В этом случае из-за несовершенной взаимодополняемости (постоянная эластичность меньше 1 и равна 0,735) наличные средства и ЦТ движутся синхронно, в связи с чем ликвидность в экономике реагирует сильнее. То есть, когда меняется базовая ставка, также меняются издержки хранения активов в наличных средствах и ЦТ.

Поэтому изменение базовой ставки приводит к изменению объемов денежных средств и ЦТ необходимых домохозяйствам.

Это взаимодополняемые виды инструментов, поэтому изменение в одном подстегивает изменение в другом инструменте в одинаковом направлении, т.е. создается эффект обратной связи (feedback effect). Другими словами, когда НБРК меняет базовую ставку, объем ликвидности меняется сильнее из-за взаимодополняемости денежных средств и ЦТ. В результате банки реагируют, меняя ставки по кредитам в большей степени, что приводит к более выраженным изменениям в потреблении и инвестициях. В свою очередь, это приводит к более выраженной реакции ВВП и инфляции в экономике.

Усиление реакции макроэкономических переменных на базовую ставку означает, что при внедрении ЦТ НБРК может оказывать большее влияние на экономику.

Кроме того, была проведена оценка экономического эффекта – изменения благосостояния людей в экономике с ЦТ и без ЦТ. При оценке коэффициента постоянной эластичности замещения учитываются удобства использования ЦТ, т.е. возможность оффлайн-оплаты ЦТ, программирования, которая далее используется в DSGE-моделях. Это означает, что все характеристики ЦТ, которые измерены данными опросов, заложены в оцененном значении коэффициента эластичности замещения между ЦТ и денежными средствами. Оценка показала нейтральный эффект, то есть благосостояние людей не меняется. Респонденты в Казахстане рассматривают ЦТ как денежные средства для проведения транзакций.

Выводы и оценки

В среднем за месяц обычный пользователь готов держать от 10 до 24% средств в ЦТ

Сценарный анализ с точки зрения макроэкономической стабильности показал оптимальный сценарий внедрения ЦТ: без начисления процентов

Пользователи не готовы полностью заменить средства на текущих счетах на ЦТ, взаимозаменяемость составила только 0,609

Доходность банковского сектора не меняется, поэтому отсутствуют риски финансовой стабильности

Анализ результатов оценки спроса выявил, что в среднем за месяц обычный пользователь готов держать **от 10 до 24% средств в ЦТ**. Вероятность принятия ЦТ населением – 67%. При этом оценка по экономическому эффекту – изменение благосостояния людей от новых выгод внедрения ЦТ – показал нейтральный эффект. Благосостояние людей не изменилось при сценарном анализе с внедрением ЦТ.

Сценарный анализ с точки зрения макроэкономической стабильности показал оптимальный сценарий внедрения ЦТ: без начисления процентов, где спрос будет от **5,7 % до 6,2% ВВП в долгосрочной перспективе**.

Анализ результатов экономических рисков показал, что риски перетока средств на текущих счетах в ЦТ контролируемы. Пользователи не готовы полностью заменить средства на текущих счетах на ЦТ, взаимозаменяемость составила только 0,609.

Внедрение ЦТ влияет на структуру наличных средств и средств на текущих счетах населения, которые не являются источником фондирования для выдачи кредитов. С этой точки зрения ЦТ не оказывает влияния на процесс формирования прибыли и капитал БВУ. В оптимальном сценарии доходность банковского сектора не меняется, поэтому отсутствуют риски финансовой стабильности.

Усиление реакции макроэкономических переменных на базовую ставку означает, что при внедрении ЦТ центральный банк может оказывать большее влияние на экономику.

Представленные выше выводы указывают на то, что процесс эмиссии и использования ЦТ в качестве третьей формы расчета в Казахстане (наряду с наличными и безналичными средствами) не будет являться источником рисков как для устойчивости денежно-кредитной политики и каналов ее трансмиссионного механизма, так и для стабильности финансовой системы.

ЭКОСИСТЕМА

60-70
стр.

Дизайн ЦТ

Потенциальные выгоды от внедрения ЦТ реализуемы только при широком принятии цифровой валюты населением как инструмента платежа

Потенциальные выгоды от внедрения ЦТ реализуемы только при широком принятии цифровой валюты населением как инструмента платежа. Об этом достаточно ясно свидетельствует пример Эквадора: главной причиной остановки разработки Dinero Electrónico был низкий уровень принятия цифровой валюты населением и участниками рынка [32]. С точки зрения экосистемы основная ценность функционала ЦТ достигается только при условии определения преимущества для конечного потребителя. Внедрение платёжной инфраструктуры ЦТ как концепции рассматривается через призму трех уровней, и по всем из них работа ведется с начала проекта.

Основные выгоды для потребителей – добавленная стоимость от новых сервисов и продуктов – определяются на самом верхнем уровне инфраструктуры

1. С 2021 года ведутся работы для разработки фундамента системы для обеспечения соответствия всем основным требованиям к национальной платёжной системе. Это базовый слой – предоставление основной равнодоступной инфраструктуры для проведения транзакций с ЦТ.
2. На основе базового слоя предоставляются новые возможности для всех участников системы – надстройки. Это дополнительные сервисы и инновационная функциональность, которая определяется наиболее важными свойствами ЦТ, такими как офлайн-сценарии, программируемость, анонимность и адресность.
3. Основные выгоды для потребителей – добавленная стоимость от новых сервисов и продуктов – определяются на самом верхнем уровне инфраструктуры. Разработка уникальных сценариев с применением ЦТ происходит в период формирования экосистемы и формулирования взаимовыгодных правил для всех участников.

Правильный выбор первоначальных бизнес-кейсов может стать ключевым драйвером создания экосистемы для поэтапного внедрения ЦТ

Двухуровневая модель обеспечивает стимулирование создания инновационных сценариев участниками, которые знают существующие проблемы потребителей. Правильный выбор первоначальных бизнес-кейсов может стать ключевым драйвером создания экосистемы для поэтапного внедрения ЦТ. Такие сценарии должны обеспечить получение сетевых эффектов, стимулировать спрос на ЦТ и, следовательно, создать рынок для поставщиков платёжных сервисов. По этой причине в ходе работ было уделено большое внимание поиску подобных бизнес-кейсов, о котором будет рассказано ниже.

CANVAS ЦТ

Новая инфраструктура ЦТ с общими сервисами наложения с добавленной стоимостью будет способствовать развитию новых услуг рыночной экосистемой

Слои инфраструктуры



Гипотезы и вопросы исследования

Оценка готовности рынка и потребителей

Для формирования всех вышеописанных уровней системы необходимо проводить поэтапную работу по вовлечению участников рынка. На стадии исследования для оценки готовности рынка принять ЦТ были сформулированы следующие вопросы:

1. Насколько хорошо участники рынка понимают концепцию ЦТ?
2. Насколько участники рынка заинтересованы в дальнейшем развитии ЦТ?
3. Какой процент сценариев можно будет отработать в рамках DT Hub?

Ниже предоставлена информация о том, с помощью каких инструментов производился поиск ответов на эти вопросы, а также сами результаты анализа.

Подход к оценке

Основными инструментами проверки готовности рынка и потребителей были

- опросы участников рынка и потребителей по ключевым темам, связанным с дальнейшим развитием и использованием ЦТ (также использовался в разделе «Экономика»)
- вовлечение участников рынка в совместную разработку сценариев в рамках пилота
- взаимодействие с участниками рынка в рамках DT Hub

Результаты исследования

Насколько хорошо участники рынка понимают концепцию ЦТ?

Ранее упоминавшийся опрос участников рынка и потребителей позволил выяснить средний уровень погруженности в вопросы, связанные с потенциальным внедрением ЦТ. В частности, с помощью данных опроса удалось определить уровень осведомлённости о ЦТ.

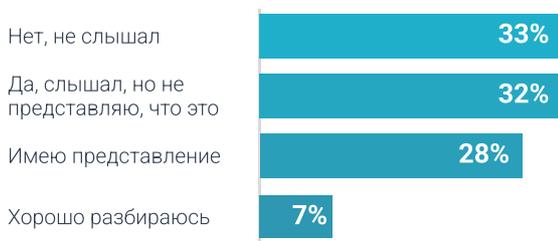


Диаграмма выше показывает, что в той или иной степени информацией о цифровой валюте в Казахстане владеют чуть больше трети потребителей (35%). Поверхностное понимание концепции ЦТ есть у 32%, в то время как ничего не знают о ней 33%. Подобный уровень осведомлённости демонстрирует необходимость дальнейших разъяснительных работ для широких аудиторий, поскольку именно уровень осведомлённости влияет на степень принятия. Методология опроса предполагала уже описанный ранее в разделе “Экономика” эксперимент - респондентам дважды задавали вопрос «Если бы завтра в Казахстане ввели цифровой тенге, насколько вероятно, что Вы бы

стали им пользоваться?», в середине и в конце опроса. Второй раз вопрос задавался уже после представления респонденту краткой информации о том, что такое ЦТ и каковы его основные характеристики. Данные показывают, что до разъяснения процент опрошенных, готовых к использованию ЦТ, был равен 60%, но после предоставления краткой справки о ЦТ значение выросло до 68% (см. инфографику).

В силу новизны темы цифровой валюты в Казахстане и относительно большого количества неосведомлённых потребителей можно заявить о том, что **для повышения принятия концепции ЦТ необходим ряд работ по разъяснению свойств ЦТ и популяризации ЦТ как платёжного инструмента.**

Отдельно стоит отметить отношение респондентов к свойствам ЦТ. Приведенная ниже диаграмма демонстрирует, какие именно характеристики цифровой валюты являются наиболее важными для потребителей.

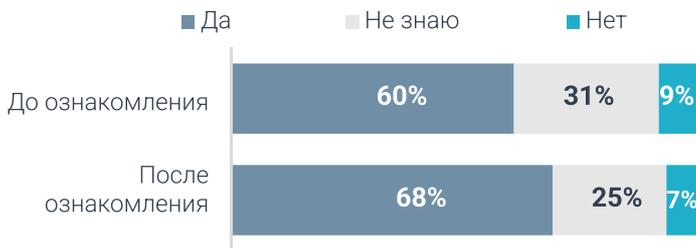
Как можно заметить, принятие населением ЦТ в первую очередь зависит от степени распространённости возможности оплачивать им товары и услуги. Этот запрос не только занимает первое место в списке качеств, которыми должен обладать ЦТ по мнению опрошенных, но и отражен в виде главного плюса наличных денег и одного из основных препятствий для безналичных платежей.

Вторым по значимости для потребителей свойством ЦТ является безопасность, что также подтверждается и тем, что технические сбои могут быть одними из главных минусов текущих безналичных методов. На третьем месте респондентами отнесена возможность оплаты без комиссии, которая на данный момент находится в разработке (см. раздел «Операционная модель»). Четвертое место занимает возможность проведения оплаты без доступа к Интернету. Данная проблема может быть решена как и с помощью методов квази-офлайн-платежей (то есть с использованием не предназначенных для этого инструментов коммуникации вроде USSD-кодов или

3000 респондентов

Все 17 регионов РК

«Если бы завтра в Казахстане ввели цифровой тенге, стали бы Вы им пользоваться?»



Готовность использовать ЦТ выше среди

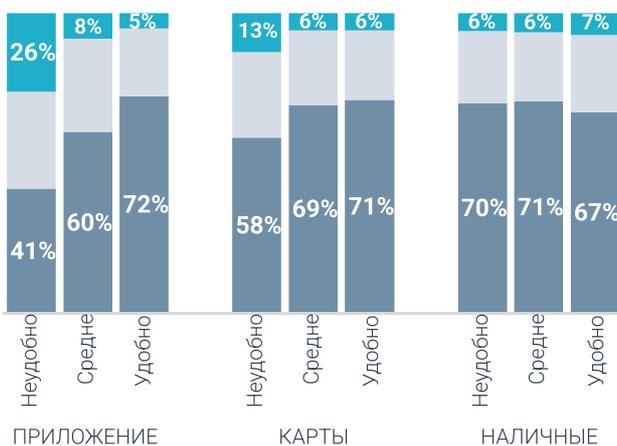
- лиц с доходами свыше 500 тыс. тенге в месяц - 79%
- казахоязычных респондентов - 71%
- студентов - 68%
- собственников бизнеса - 68%
- самозанятых - 65%
- мужчин - 65%
- молодежи - 62%
- ежедневно использующих приложение банка - 65%
- ежедневно использующих мобильные платежные сервисы - 74%

Не готовы использовать ЦТ наиболее уязвимые слои общества

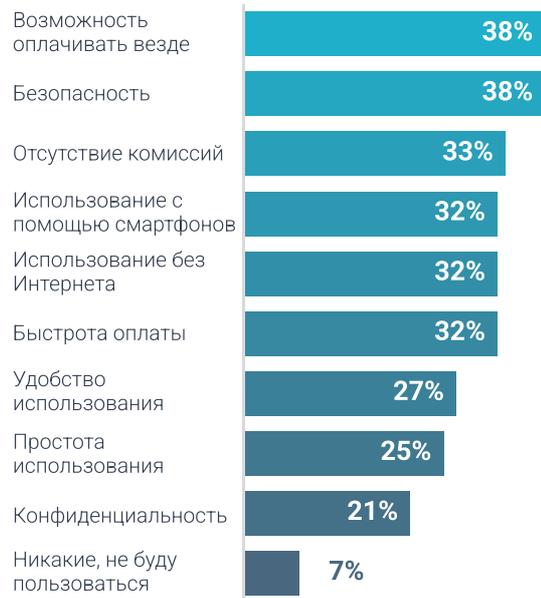
- малообеспеченные с доходами до 50 тыс. тенге в месяц - 12%
- пенсионеров - 15%
- инвалидов - 13%
- людей старшего поколения в возрасте 51+ - 11%
- людей со средним образованием или ниже - 11%

Наименее готовые к использованию ЦТ те, кто ощущает неудобство при использовании безналичных методов

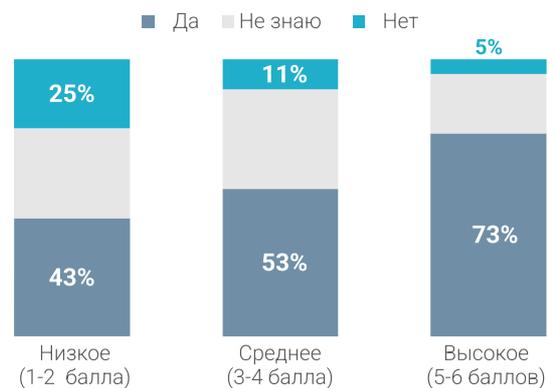
Принятие ЦТ после заметки о ЦТ в зависимости от удобства методов оплаты



Наиболее важные характеристики ЦТ

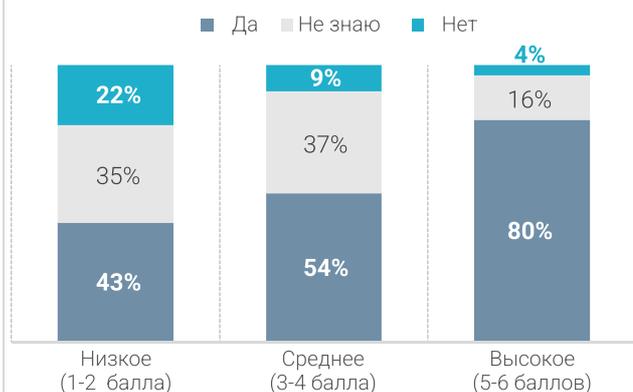


Принятие ЦТ после разъяснения в зависимости от степени доверия своему банку



СТЕПЕНЬ ДОВЕРИЯ СВОЕМУ БАНКУ

Принятие ЦТ после разъяснения в зависимости от степени доверия НБРК



СТЕПЕНЬ ДОВЕРИЯ НБРК

2G-протоколов), так и с помощью реализации полноценной цепочки платежей в оффлайн-режиме. Наконец, потребителям также важны такие качества ЦТ как простота, удобство и скорость. Как показывают результаты опроса, все эти три качества могут быть отнесены как к наличным деньгам, так и к безналичным методам.

Насколько участники рынка заинтересованы в дальнейшем развитии ЦТ и какой процент сценариев можно будет отработать в рамках DT Hub?

В подходе к оценке потенциала формирования экосистемы ЦТ особое внимание уделялось открытой коммуникации с рынком и всестороннему вовлечению в процесс исследования. С начала текущего года были проведены ряд встреч и дизайн-сессий – в частности, в ходе таких встреч представлены итоги пилотного проекта Цифровой тенге за 2021 год и обозначены цели и задачи второй фазы пилотирования на 2022 год.

Для активного взаимодействия участников финансового рынка, независимых экспертов, технологических провайдеров и международных партнеров, а также в целях развития экосистемы ЦТ в июне текущего года была создана коллаборативная площадка Digital Tenge Hub. На её базе проводились все коммуникации и взаимодействия всех стейкхолдеров для совместного исследования вопросов внедрения национальной цифровой валюты и её дальнейшего развития. Например, в рамках функционирования DT Hub заключены меморандумы о сотрудничестве с Digital Euro Association и Национальным Банком Кыргызской Республики, а также с рядом технологических провайдеров.

Участие в деятельности площадки дарует ряд преимуществ – возможность создания новых экспериментальных сервисов на платформе ЦТ для привлечения новых клиентов, разработка тестовых смарт-контрактов, обучение разработчиков по международным стандартам, обмен опытом, получение консультаций от зарубежных партнеров и экспертов, а также доступ в технологическую песочницу ЦТ для

экспериментов и совместные изучения сценариев (case studies) для проработки технологических вопросов ЦВЦБ.

Одним из наиболее важных мероприятий на базе DT Hub являлся конкурс идей Ideathon, проведенный в целях определения ценностного предложения для конечного потребителя совместно с участниками рынка. Основной целью конкурса являлось понимание уровня заинтересованности и осведомленности рынка о новых возможностях платёжных сценариев с применением ЦТ. По результатам конкурса участники рынка предложили 17 инновационных сервисов для возможной реализации на платформе ЦТ. Первоначальный анализ поступивших заявок по конкурсу Ideathon был проведён согласно следующим критериям:

- выгоды для потребителя
- выгоды для государства и бизнеса
- новизна сценария по сравнению с текущими сценариями на рынке
- применение свойств программирования ЦТ
- сохранение двухуровневой модели платежной системы
- соответствие требованиям смарт-контракта

Поступившие заявки были распределены по трём группам. Основными критериями для отбора участников в первой группе стали возможная скорость их реализации и функционал, необходимый для разработки сценариев. Во вторую группу вошли сценарии со стратегическими выгодами для государства, бизнеса и населения, а также перспективами развития экосистемы ЦТ за пределами платежно-расчетного функционала. В третью группу вошли проекты, которые могут продемонстрировать возможности программирования и расширяют спектр сценариев для применения ЦТ в платежно-расчетной инфраструктуре.

Сценарий расчета по сделкам между юридическими лицами



ОГРАНИЧЕНИЯ

Зависимость от рабочих часов БВУ

Длительность операций

Риск кассового разрыва

Риск срыва сроков по сделкам



ПРЕИМУЩЕСТВА

Моментальный расчет

Возможность проведения платежей 24/7/365

Отсутствие задержек по срокам сделки

Маркировка токенов

Сценарий автоматизации сферы аренды

АРЕНДАТОР



АРЕНДОДАТЕЛЬ



ОПЛАТА НАПРЯМУЮ

ПОВЫШЕННЫЕ РИСКИ

Отсутствие финансовых обязательств

Отсутствие юридических обязательств

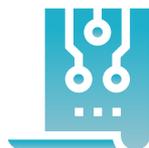
Отсутствие гарантий

Нерегулируемый рост цен

АРЕНДАТОР



СМАРТ-КОНТРАКТ
СТРАХОВАНИЕ



СПУ



АРЕНДОДАТЕЛЬ



ПРИЕМУЩЕСТВА

Гарантия платежеспособности клиента

Своевременная оплата

Автоматизация процесса

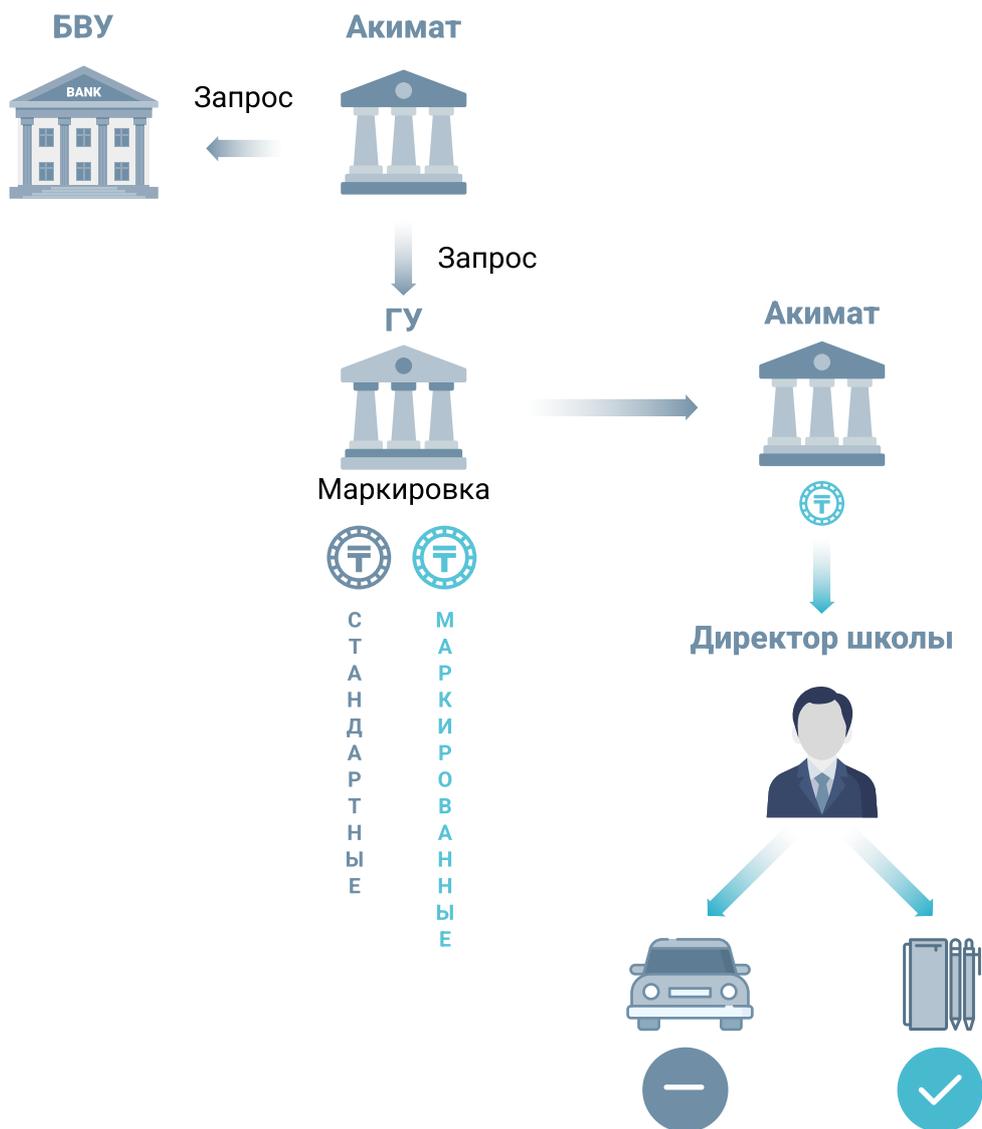
Отсрочка платежа

Страхование от форс-мажора

Страховое удержание с обеих сторон:

- Компенсация убытков Арендодателя
- Гарантия сделки Арендатору

Сценарий «Система получения социальной помощи для СУСН»



ПРЕИМУЩЕСТВА

Получение своевременной социальной помощи по принципу «единого окна»

Маркировка токенов (использование средств по целевому назначению)

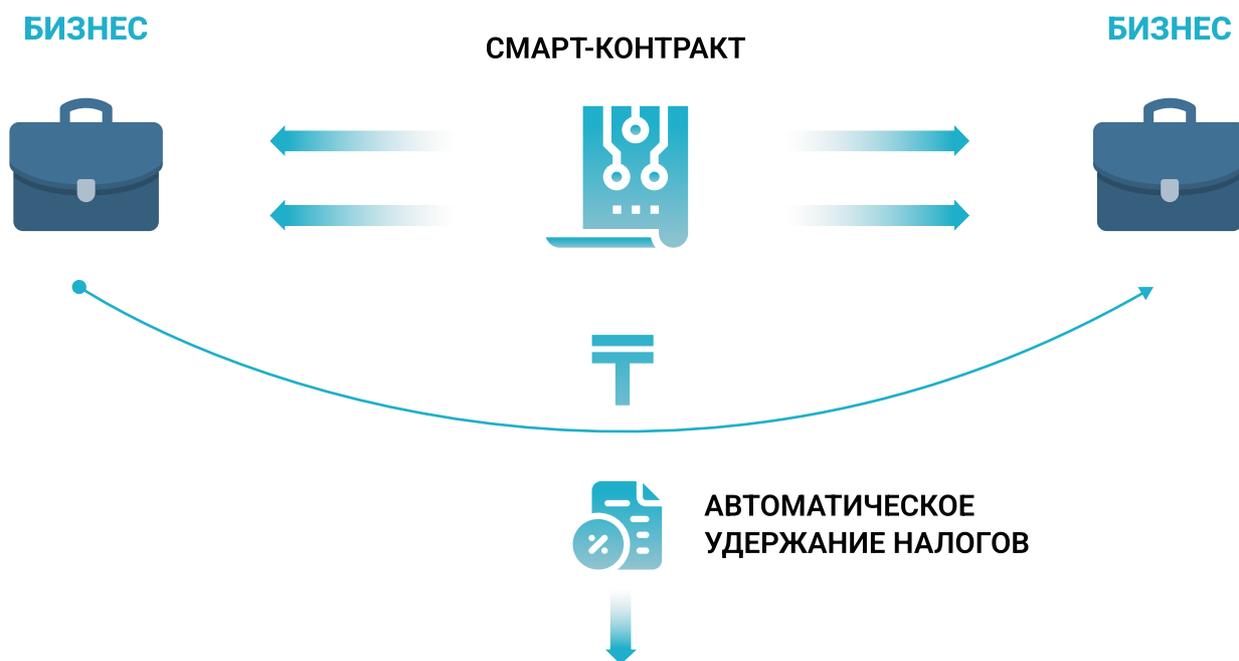
Автоматизация процесса

Прозрачность процессов социальной помощи

Цифровая трансформация текущих процессов

Отсутствие необходимости создания дополнительного специального счета
(маркированные и стандартные токены хранятся в едином кошельке)

Сценарий «Автоматизация налоговых платежей»



ПРЕИМУЩЕСТВА

Автоматический расчет и оплата налогов

Автоматизированная работа бизнеса и государственных органов

Возможность выбора налогового режима

Упрощение ведения бизнеса

Отсутствие налоговых задолженностей

Среди предложенных инициатив имеются перспективные сценарии по автоматизации налоговой отчетности с помощью новых смарт-контрактов. Другой заслуживающей внимания идеей является реализация автоматизированного рекрутингового сервиса на блокчейне, обеспечивающая все измеряемые условия и договоренности. Кроме того, этот сервис создает информацию о спросе и предложении (вакансии) в виде смарт-контракта. Выплаты и налоги в этом сервисе защищены автоматическими смарт-контрактами в связке с DLT, что несет стратегические выгоды для населения, государства и бизнеса.

Также получены инновационные предложения по решению задач в области заключения договоров аренды, найма и оказания услуг с использованием DLT-технологий. Один из сценариев фокусировался на создании экосистемы в виде единой цифровой платформы для автоматизации, регистрации и цифровизации всех процессов индустрии аренды в РК. Предложения по выплате заработной платы в ЦТ позволяли в теории автоматизировать процессы и снизить вероятность возникновения ошибок расчета. Другим многообещающим сценарием, предложенным участником рынка, оказался бизнес-кейс «Сценарий расчета по сделкам между юридическими лицами» - возможность мгновенного расчёта в режиме 24/7/365 создаёт уникальную ценность для большого количества потребителей. Более подробно об этих и других сценариях можно узнать в инфографиках данного раздела.

Сценарий «Безопасная сделка»

01

ЗАКАЗЧИК

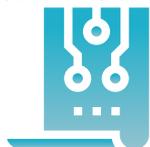


02

ЗАКАЗЧИК



СМАРТ-КОНТРАКТ



03

ИСПОЛНИТЕЛЬ



ПРЕИМУЩЕСТВА

Защита расчетов между участниками

Прозрачность всех этапов сделки

Гарантия выплаты в срок

Полная/частичная автоматизация сделки

Упрощение процесса сбора налогов

Уменьшение конфликтных ситуаций

НБРК реализовал сценарий, занявший первое место среди участников первой группы, а именно сценарий «Безопасная сделка» для автоматизации расчетов по фриланс-услугам, и проводит обучающие сессии по результатам разработки и реализации смарт-контрактов.

Автоматический
расчет

Автоматический
вычет налогов

Сценарий «Безопасная сделка» — это инструмент, который помогает защитить расчеты между участниками. Все этапы безопасной сделки и использования ЦТ максимально прозрачны: исполнитель уверен в том, что у заказчика есть денежные средства на оплату заказа, заказчик контролирует факт выплаты на счёт исполнителя. Сделка может быть частично автоматизирована: например, выплата может происходить автоматически по истечении определённого времени. Для государства сервис безопасной сделки может упростить процесс сбора налогов и уменьшить количество конфликтных ситуаций.

У участников рынка существует стабильный интерес к платформе ЦТ

Результаты проведенного Ideathon'a демонстрируют, что у участников рынка существует стабильный интерес к платформе ЦТ. Даже в условиях крайне сжатого времени проведения конкурса (14 дней) и упоминаемым выше относительно невысоким уровнем осведомленности о ЦТ участниками рынка были представлены 17 возможных инновационных сценариев использования платформы цифровой валюты. Отдельно стоит отметить тренд на повышение осведомленности среди представителей финтех-рынка. В сравнении с данными интервью представителей БВУ 2021 года можно заметить, что уровень погруженности в вопросы, связанные с перспективами казахстанской ЦВЦБ, значительно увеличился.

В ходе работ прошлого года по изучению фундамента для возможной экосистемы ЦТ собраны 60 наиболее актуальных вопросов от представителей БВУ. Ответы на них были разосланы БВУ и продемонстрированы на встрече 17 сентября 2021 года с последующим обсуждением.

Выводы и оценки

Совокупность всех вышеизложенных факторов и ответов на заданные в Модели вопросы позволяет присвоить платформе ЦТ по аспекту «Экосистема» **оценку «С»** (больше половины участников рынка и потребителей готова и заинтересована во внедрении и дальнейшем развитии ЦТ). Для достижения более высоких значений необходимо проведение работ по повышению уровню осведомлённости среди потребителей и участников рынка, а также продолжение развитие экосистемы посредством мероприятий и встреч на площадке DT Hub. При этом также стоит отметить повышение уровня осведомлённости и эффективность функционирования DT Hub в этом году, что в свою очередь позволяет заявить о перспективности дальнейших действий по взаимодействию с участниками рынка.

Больше половины участников рынка и потребителей готова и заинтересована во внедрении и дальнейшем развитии ЦТ

Необходимо проведение работ по повышению уровню осведомлённости среди потребителей и участников рынка

ОПЕРАЦИОННАЯ МОДЕЛЬ

72-82

стр.

Дизайн ЦТ

Операционная модель ЦТ – это комплекс бизнес-процессов, процедур и регламентов

Операционная модель ЦТ – это комплекс бизнес-процессов, процедур и регламентов, направленный на юридически определенное, бесперебойное и взаимовыгодное взаимодействие участников системы.

В зависимости от мотивов каждой конкретной юрисдикции при внедрении ЦВЦБ, распределение ролей в операционной модели будет отличаться, что потребует проведения обсуждений с пользователями и заинтересованными сторонами. Но общемировой консенсус заключается в том, что операционная совместимость ЦВЦБ на национальном уровне будет иметь ключевое значение для эффективной работы системы. Интероперабельность обеспечит сосуществование системы ЦВЦБ с другими национальными платежными системами и будет способствовать более широкой доступности, устойчивости и разнообразию платежных сервисов.

Устойчивое развитие экосистемы и достижение заявленных преимуществ ЦТ возможно только при условии вовлеченности участников рынка и широкого проникновения в среду потребителей

Устойчивое развитие экосистемы и достижение заявленных преимуществ ЦТ в условиях двухуровневой архитектуры возможно только при условии вовлеченности участников рынка и широкого проникновения в среду потребителей.

Гипотезы и вопросы исследования

Операционная модель состоит из следующих составляющих, которые необходимо определить в рамках исследования:

1. Распределение ролей, прав, обязанностей участников платформы ЦТ, требования к участникам
2. Бизнес-модель платформы и подходы к тарификации
3. Комплекс мер и подходов по управлению диспутами
4. Подходы к модели учета ЦТ
5. Подходы к организации соответствия требованиям ПОД/ФТ
6. Закрепление вышеуказанных подходов в соответствии с НПА
7. Модель и подходы достижения оптимального уровня проникновения ЦТ

Подход к оценке

Ответы на вопросы операционной модели сформированы по результатам обсуждений с участниками рынка на базе DT Hub и анализа международных исследований.

Результаты исследования

1. Распределение ролей, прав, обязанностей участников платформы ЦТ, требования к участникам

Предлагаемая операционная модель опирается на существующую двухуровневую архитектуру, где НБРК эмитирует ЦТ, платежные провайдеры открывают кошельки и распределяют ЦТ по требованию потребителя. Описываемая модель позволяет добиться решения целого ряда задач – повышение финансовой инклюзивности и сохранение финансовой стабильности. Она также позволяет получить БВУ/ФО доступ к новым доходам, что, в свою очередь, приведет к новому эволюционному этапу развития финансового рынка в стране. Согласно обзору БМР, предложено базовое распределение ролей в системе ЦТ [35].

	Перечень ролей	Базовое распределение функций и задач
1	НБРК – оператор платформы	<p>Основное руководство</p> <p>Основные принципы операций с ЦТ/использования ЦТ, определяющие правовую основу, общее управление, управление рисками, доступ и другие требования к участникам</p> <p>Базовая инфраструктура</p> <p>Выпуск, погашение и расчеты с ЦТ в основном реестре, мониторинг, обеспечение гарантий</p> <p>Инфраструктура обработки</p> <p>Подготовка, обработка и реконсилияция, связь с основной инфраструктурой, связь с вспомогательными функциями (например, системы цифровой идентификации, базовые телекоммуникационные сети)</p>
2	Провайдеры платежных услуг	<p>Услуги по обработке</p> <p>Предварительные проверки платежей (например, проверка лимитов, наличие средств)</p> <p>Авторизация, верификация или валидация (например, управление исключениями, восстановление и исправление транзакций, обработка лимитов авторизации во время оффлайн)</p> <p>Проверка (например, безопасность и нормативные проверки) Данные и аналитические услуги</p> <p>Платежные услуги (взаимодействие с конечными пользователями)</p> <p>До транзакции: например, устройство доступа или канал, регистрация пользователей</p> <p>Транзакция: например, платежная инструкция, аутентификация, обслуживание клиентов и поддержка</p>

Перечень ролей	Базовое распределение функций и задач
<p>2 Провайдеры платежных услуг</p>	<p>После транзакции: например, платежное уведомление, выписки и выставление счетов</p> <p>Организация сценариев</p> <p>Набор бизнес- и технических правил, определяющих, как работает сценарий использования</p>
<p>3 Уполномоченный орган в сфере ПОДУФТ</p>	<p>Инфраструктура обработки</p> <p>Связь со вспомогательными функциями (например, системы цифровой идентификации, базовые телекоммуникационные сети)</p>
<p>4 ГУ в части программирования токенов</p>	<p>Организация сценариев</p> <p>Набор бизнес- и технических правил, определяющих, как работает сценарий использования</p>

Распределение функций и задач между ролями может различаться в зависимости от сценария использования ЦТ

Подход к разработке требований аналогичен системно значимым платежным системам. Описанная операционная модель не требует издержек для подключения к платформе ЦТ больше, чем существующие механизмы и нормы.

Распределение функций и задач между ролями может различаться в зависимости от сценария использования ЦТ. Результаты пилота показали минимальные издержки для интеграции с платформой ЦТ на стороне участников рынка (минимум доработок).

Независимо от дизайна разработка и запуск системы ЦВЦБ будет сложной задачей для любого ЦБ. Любые функции, переданные на аутсорсинг, должны быть тщательно проработаны для обеспечения общественного доверия к системе ЦВЦБ. Аналогичным образом потребуется индивидуальный и коллективный надзор за функциями и услугами, предоставляемыми или управляемыми частными посредниками.

Требуется детализация распределения ролей и функций с учетом запланированных задач при реализации сценариев 2023 года

Требуется детализация распределения ролей и функций с учетом запланированных задач при реализации сценариев 2023 года. Предполагается отработать предлагаемые подходы в рамках регуляторной песочницы НБРК совместно со всеми участниками рынка.

	Эмиссия		Валидация		Обновление реестра		КУС-ПОД/ФТ		Пользовательский интерфейс		Данные пользователя		Обслуживание клиентов	
	Владелец	Исполнитель	Владелец	Исполнитель	Владелец	Исполнитель	Владелец	Исполнитель	Владелец	Исполнитель	Владелец	Исполнитель	Владелец	Исполнитель
 Багамы														
 Канада														
 Китай														
 ВКВС														
 Швеция														
 Уругвай														

Цветовая схема

Центральный Банк
 Оба
 Частный
 В стадии исследования

Источник: МВФ [33]

ВКВС- Восточно-Карибский валютный союз

2. Бизнес-модель платформы и подходы к тарификации

Подходы зарубежных регуляторов

Был сделан обзор ряда проектов ЦВЦБ разных стран:

ЦБ Багамских островов (где цифровая валюта запущена), Народного банка Китая, Восточно-Карибского ЦБ и ЦБ Уругвая (где проведены и дальше продолжают пилоты с участием реальных потребителей и ТСП), Риксбанка (где ЦВЦБ анализируется правительственными или парламентскими органами вне центрального банка), Банка Канады (где ЦБ осуществил проект ЦВЦБ и решил пока не выпускать цифровую валюту).

Обзор позволил сделать следующие выводы о подходах зарубежных регуляторов [33].

Важную роль в любой экосистеме будет играть доступ к платежным данным и их обработка. Вопросы конфиденциальности могут создать ряд других проблем, связанных с проектированием и совместимостью, начиная от используемых стандартов обмена сообщениями, создания стимулов для различных посредников предлагать услуги, а также взаимодействия с традиционными системами, которым требуется подробная информация о счетах и транзакциях [36].

Народный банк Китая не взимает плату с посредников или пользователей, а посредники не могут взимать плату с отдельных пользователей в рамках проекта e-CNY. Однако посредники могут взимать плату с ТСП. Народный банк Китая считает, что это является существенным стимулом для входа на рынок при контроле суммы сборов.

Банк Канады утверждает, что выбор бизнес-модели является сложным. Один из возможных вариантов: ЦБ сам предоставляет базовую платежную функцию ЦВЦБ для населения, возможно, но не обязательно взимая плату за ее использование. Риксбанк также рассматривает данный подход.

Вопрос о том, должен ли ЦБ взимать плату с посредников за использование системы ЦВЦБ, также связан с вопросом о том, ожидает ли он возмещения своих расходов на разработку. Существует риск того, что, если ЦБ будут взимать сборы, то посредники со своей стороны переложат издержки на конечных потребителей и повысят платежи, что может противоречить первоначальным целям политики. Вопрос о том, покрывать ли расходы и каким образом, остается открытым, банк считает одной из наиболее важных областей своих исследований.

Сотрудники Риксбанка также заявляют, что взимание платы с посредников затруднено из-за существующей нормативной базы. Другой вопрос заключается в том, что взимание комиссии может противоречить обязательству банка предлагать платежи как общественное благо. Доходы ЦБ, скорее всего, будут поступать исключительно в виде сеньоража.

Субсидирование внедрения ЦВЦБ в настоящее время не рассматривается многими ЦБ, но Риксбанк обсуждает возможность субсидирования затрат на разработку определенных функций, которые частный сектор не сочтет прибыльными. В качестве примера можно привести повышение устойчивости/бесперебойности платежей и разработку платежных решений для меньшинства.

НБРК определил следующие основные принципы в разработке бизнес-модели:

- 1. НБРК не заинтересован в прибыли, бизнес-модель должна покрывать только расходы на содержание.**
- 2. Подходы к тарификации должны быть выработаны на принципах взаимовыгодности всех участников платформы.**

В целях определения оптимальной операционной модели, согласно описанным принципам, в 2023 году в регуляторной песочнице планируется выработать правила бизнес-модели ЦТ совместно со всеми участниками.

3. Комплекс мер и подходов по управлению диспутами

Обеспечение интересов конечных пользователей – ключевая основа любой платежной системы. Важно обеспечить гарантии потребителям в различных сценариях. Участникам необходимо рассмотреть новые способы обеспечения защиты потребителей при осуществлении платежей с ЦТ [36]:

- несанкционированный платеж (например, если цифровой токен украден или утерян)
- мошенничество, причиняющее вред клиенту
- недоработки, сбои в услуге, предоставляемой частным сектором
- дефекты приобретенных товаров или услуг

Необходимо проработать в рамках тестов в регуляторной песочнице вопросы, связанные с:

- затратами на расследования и разрешения претензий и споров
- расходами на функционирование системы защиты прав потребителей

На базе ролевой модели операционной модели ЦТ будет выработана таксономия и алгоритмы разрешения диспутов. Система будет автоматизирована.

4. Подходы к модели учета ЦТ

Модель учета /денежная схема – один из способов записи и сохранения состояния транзакции. Определены восемь вариантов денежной схемы проведения расчетов.

Денежная единица	Стоимость	Предъявитель	Идентификация единицы	Разъяснение
Тривиальная	фиксированная	фиксированный	фиксированная	Тривиальная схема очень проста: ничто не может измениться, поэтому никакие платежи невозможны
Вексель	фиксированная	переменный	фиксированная	Платеж по вексельной схеме заключается в смене предъявителя. Банкнота номиналом €20 с уникальным серийным номером передается от Алисы к Бобу или право собственности на цифровую купюру в €20 переходит от Алисы к Бобу
Счет	переменная	фиксированный	фиксированная	Оплата по схеме счета состоит в изменении стоимости единиц с фиксированными предъявителями. Счет Алисы дебетуется на €20, счет Боба кредитуется на €20
UTXO	переменная	переменный	переменная	<p>UTXO расходуются только один раз. В момент, когда это происходит, создаются новые UTXO с разными идентификаторами.</p> <p>Существующий UTXO Алисы уничтожается, создавая два новых UTXO, один из которых принадлежит Алисе, второй новый UTXO стоимостью €20, принадлежит Бобу</p>
Расширенные счета	переменная	переменный	фиксированная	Право собственности на счета может меняться
Вариант 1	фиксированная	фиксированный	переменная	Эта схема не допускает изменения ни стоимости, ни владельца денежной единицы, поэтому оплата по этой схеме невозможна
Вариант 2	фиксированная	переменный	переменная	Эта схема похожа на схему купюр, но серийный номер купюры меняется при ее расходовании; она не предлагает дополнительных преимуществ по сравнению с вексельной схемой
Вариант 3	переменная	фиксированный	переменная	Эта схема похожа на схему счета, но каждый платеж приводит к созданию нового счета. Она не предлагает ничего большего, чем счет с фиксированным идентификатором

И счета, и векселя имеют конкретные идентификационные номера с серийными номерами, которые не меняются во время проведения платежа.

По ЦВЦБ рассматриваются следующие три вида [33]

Категории	Варианты
Денежная схема (модель учета)	Счет, УТХО, вексель
Тип учетной книги	Доверенные машины, открытый блокчейн, закрытый DLT, централизованный блокчейн, офлайн
Механизм передачи/чек на предъявителя	Аутентификация на основе идентификационных данных, аутентификация на основе токенов или подписей, смарт-контракты

Модели учета могут влиять на многие элементы ЦТ, включая масштабируемость, анонимность, правовой статус денежной единицы и безопасность денежной массы. Однако существуют характеристики ЦВЦБ, которые часто упоминаются в контексте токенов или счетов и на которые выбор модели учета не влияет, включая доступность и устойчивость системы, конфиденциальность и безопасность бухгалтерской книги. Они вытекают из выбора технологии на предъявителя или типа бухгалтерской книги.

Для ЦТ была выбрана модель учета УТХО в связи с преимуществами в части анонимности, программирования в сравнении с другими вариантами учета. Модель балансового учета подробно расписана в [Итоговом докладе 2021 года](#).

Категории	Разъяснение
Масштабируемость и время расчетов	Выбор денежной схемы влияет на масштабируемость платежей и определяет процесс, с помощью которого происходит расчет. Леджер и технология на предъявителя технологии также оказывают сильное влияние на масштабируемость и время расчетов
Анонимность	Счет содержит историю нескольких транзакций одного и того же пользователя, что облегчает использование различных аналитических методов для деанонимизации личности владельца счета. Если деанонимизировать одну транзакцию, можно определить всю историю платежей этого пользователя
	Вексели и УТХО облегчают применение техник, позволяющих сохранить личность в тайне, таких как разделение транзакций и одноразовые адреса
Правовой статус	Некоторые существующие правовые рамки для денег ЦБ проводят различия между счетами и инструментами на предъявителя или наличными. Юридический анализ, проведенный МВФ, показал, что в результате этого может быть то, что токены ЦВЦБ юридически более допустимы в некоторых юрисдикциях, чем счета, предлагаемые непосредственно населению. Необходимо провести дополнительные исследования, чтобы определить, являются ли эти различия в первую очередь функцией выбора технологии на предъявителя или денежной схемы

Категории	Разъяснение
Процентные доходы	<p>Проценты по инструментам на основе счета периодически рассчитываются из остатка</p> <p>Если УТХО или счета объединяются в кошельки, проценты могут рассчитываться на уровне кошелька аналогично тому, как рассчитываются проценты по счету</p> <p>Однако и УТХО, и векселя позволяют дополнительно рассчитывать проценты от каждой операции с единицей или рассчитывать вознаграждение от конкретного периода владения, то есть от возраста УТХО или срока, в течение которого вексель находился у предыдущего владельца</p>
Лимиты	<p>Лимиты или ограничения на владение довольно просто применить к единицам, основанным на счете, поскольку лимит просто сравнивается с балансом счета.</p> <p>Для векселей и УТХО сначала необходимо рассчитать общую стоимость владений индивидуума</p>
Программируемость	<p>Программируемые деньги возможны во всех трех денежных схемах, но характер программируемого объекта данных меняется. Для счетов программируемым является баланс, так как умный контракт осуществляет платеж с баланса. Для УТХО программируются и предъявитель, и счет, так как умный контракт выпускает новые УТХО. Для счетов программируется предъявитель, так как смарт-контракт передает счет новому владельцу</p>

Источник: Guardtime [34]

5. Подходы к организации соответствия требованиям ПОД/ФТ

Основные проблемы обеспечения интероперабельности платформы ЦВЦБ связаны с техническими, коммерческими и юридическими вопросами.

Правовые/регулятивные внутренние барьеры могут включать различия, возникающие в рамках надзора за участниками и в требованиях к соблюдению, а также в правилах окончательности расчетов и защиты прав потребителей в платежных системах. В частности, если будут существовать различные надзорные требования между ЦТ и другими системно значимыми платежными системами, то может быть недостаточное дублирование для обеспечения бесперебойного движения средств (при условии, что не будет внедрен технический интерфейс). Аналогичным образом, если требования ПОД/ФТ будут выше или будут отличаться от существующих платежных систем, это может привести к дополнительным расходам для участников. Для платежных систем могут различаться правила окончательности расчетов и защиты прав потребителей (например, если одна система работает по принципу нетто-расчетов, а другая – по принципу валовых расчетов, то процедуры в случае ошибок, задержек, мошенничества, краж или неплатежеспособности отличаются).

Для устранения барьеров крайне важно взаимодействие с другими государственными органами, на которые возложена задача надзора за банками, поставщиками платежных услуг, платежными системами. НБРК придерживается того принципа, что требования будут аналогичны к требованиям ПОД/ФТ системно значимых платежных систем.

6. Закрепление вышеуказанных подходов в соответствии с НПА

Базовые параметры операционной модели будут разработаны в следующем году. Также с учетом необходимости доработок правил взаимодействия в регуляторной песочнице будут проведены дополнительные анализы. Результаты исследования регуляторных вопросов 2022 года резюмированы в следующей главе.

7. Модель и подходы достижения оптимального уровня проникновения ЦТ

Согласно ранее описанной пирамиде Canvas, в дизайне ЦТ двухуровневая модель обеспечивает стимулирование создания таких инновационных сценариев участниками, которым известны конкретные проблемы и боли потребителей. В процессе изучения ЦТ ключевым драйвером создания экосистемы является правильный выбор первоначальных бизнес-кейсов для поэтапного внедрения ЦТ. Такие сценарии должны обеспечить сетевые эффекты, стимулировать спрос на ЦТ и, следовательно, создать рынок для поставщиков платежных сервисов.

В качестве первичных сценариев рассматриваются X2G/G2X-сценарии.

Обеспечение интероперабельности между системами участников рынка – одна из основных задач для построения эффективной операционной модели. Операционная совместимость ЦТ может способствовать конкуренции между поставщиками платежных услуг, создавать условия для инноваций и повышать операционную устойчивость национальной платежной экосистемы. Низкий уровень интероперабельности между платежными системами может привести к фрагментации платежного ландшафта на замкнутые контуры. В результате пользователи и торговцы могут столкнуться с расходами из-за участия в системах с ограничениями, что снижает скорость и повышает стоимость платежей.

Технические барьеры могут включать несогласованные стандарты форматов сообщений, элементов данных, систем нумерации и кодирования, протоколов безопасности, масштабируемости или пропускной способности и часов работы.

Решение данных вопросов возможно с помощью применения следующих методов: общие (международные) технические стандарты и/или интерфейсы прикладного программирования; требования минимально жизнеспособных стандартов безопасности или поощрение других систем к принятию более строгих стандартов безопасности; раннее и частое общение с другими системами для оценки объемов и пропускной способности; установление правил для платежей ЦТ, инициированных в часы закрытия других систем. Для выработки оптимальных подходов необходимо вовлечение всех участников системы для согласования технической спецификации системы ЦТ и координации вопросов операционной совместимости.

Коммерческие барьеры могут включать нежелание других участников использовать ЦТ для сохранения и защиты существующих доходов из-за отсутствия полного понимания возможных рисков. В ответ ЦБ может стимулировать участие в экосистеме ЦТ и проводить информационно-разъяснительную работу по всем аспектам применения ЦТ. Также снижение затрат за счет устранения вышеуказанных барьеров технической совместимости может решить данную проблему.

Выводы и оценки

Распределение функций и задач между ролями может различаться в зависимости от сценария использования ЦТ

Предлагаемая операционная модель опирается на существующую двухуровневую архитектуру, где НБРК эмитирует ЦТ, платежные провайдеры открывают кошельки и распределяют ЦТ по требованию потребителя. Распределение функций и задач между ролями может различаться в зависимости от сценария использования ЦТ. **Для ЦТ была выбрана модель учета УТХО в связи с преимуществами в части анонимности, программирования в сравнении с другими вариантами учета.**

Результаты исследования показали низкие регуляторные издержки

Результаты исследования показали низкие регуляторные издержки ввиду следующих причин:

- Технологические, регуляторные требования к участникам рынка для подключения к системе ЦТ будут аналогичны существующим требованиям системно значимых платежных платформ. Результаты пилота показали минимальные издержки для интеграции с платформой ЦТ на стороне участников рынка (минимум доработок)
- Мониторинг и надзор работы системы будут автоматизированы с применением смарт-контрактов. На базе ролевой модели операционной модели ЦТ будет выработана таксономия и алгоритмы разрешения диспутов
- Ущерб базовым бизнес-моделям БВУ не ожидается

Ущерб базовым бизнес-моделям БВУ не ожидается

Последнее возможно, так как:

- экономические исследования не демонстрируют риски перетока средств на текущих счетах в ЦТ
- имеются инструменты контроля перетоков средств в ЦТ – лимиты
- возможна коммерциализация новых услуг/продуктов с ЦТ

Стимулы для подключения к платформе ЦТ не будут затрагивать средства участников рынка.

Предполагается отработать предлагаемые подходы в рамках регуляторной песочницы НБРК совместно со всеми участниками рынка

Далее требуется детализация распределения ролей и функций с учетом запланированных задач при реализации сценариев 2023 года. Предполагается отработать предлагаемые подходы в рамках регуляторной песочницы НБРК совместно со всеми участниками рынка.

РЕГУЛИРОВАНИЕ

84-89
стр.

Дизайн ЦТ

Легальный статус ЦТ имеет ключевое значение для его функционирования в качестве компонента национальной платёжной системы, предопределяет степень принятия ЦТ населением и влияет на выбор возможных бизнес-кейсов для реализации на платформе. Однако разработка рекомендаций для внесения необходимых изменений в НПА осложняется новизной самого концепта цифровых валют : действующая законодательная база не предусматривает никаких других законных платёжных средств, кроме банкнот и монет.

В 2022 году проведены исследования соответствующих законов и кодексов РК с целью выяснения объема необходимых изменений, а также их характера. В процессе выработки механизмов регулирования были также определены следующие аспекты концепции нормативно-правовой базы ЦТ:

ЦТ должен являться законным платёжным средством на территории РК, тем самым обеспечивая повсеместный прием ЦТ к оплате за товары и услуги

1. ЦТ будет объединять в себе некоторые особенности наличных денежных средств и безналичных денежных средств
2. НБРК будет иметь исключительную компетенцию по эмиссии ЦТ и контролю над деятельностью системы ЦТ
3. Нарицательная стоимость ЦТ должна равняться нарицательной стоимости казахстанского тенге, и ЦТ должен являться законным платёжным средством на территории РК, тем самым обеспечивая повсеместный прием ЦТ к оплате за товары и услуги
4. ЦТ будет являться обязательством НБРК (будет выступать в роли гаранта)

Гипотезы и вопросы исследования

Проведенные в ходе составления операционной модели исследования позволили создать список наиболее важных вопросов, ответы на которые позволяют урегулировать наиболее принципиальные аспекты всего жизненного цикла ЦТ:

1. Какова наиболее подходящая дефиниция ЦТ?
2. Является ли ЦТ объектом вещных или обязательственных прав?
3. Что включает в себя оборот ЦТ?
4. Каков круг действующих лиц в процессе оборота ЦТ?
5. Как должно измениться восприятие персональных данных и банковской тайны в результате внедрения ЦТ?

6. Как должна разграничиваться ответственность за неправомерные действия при обороте ЦТ (административно-правовая и уголовная)?

7. Какие квалифицирующие признаки правонарушений следует выделить?

8. Как должна измениться процедура ПОД/ФТ в процессе внедрения ЦТ?

9. Какие следует установить ограничения в обороте ЦТ (по кругу лиц и характеру операции)?

Ниже представлена информация о предполагаемых изменениях в законодательстве РК, включающие в себя в том числе ответы на вышеуказанные вопросы.

Подход к оценке

Работы по созданию рекомендаций для внесения изменений в НПА состояли из следующих этапов:

- Анализ существующих подходов к созданию законодательства для полноценного функционирования ЦВЦБ
- Анализ законодательства РК на предмет его актуальности и корреляции с каждым этапом жизненного цикла ЦТ
- Разработка рекомендаций с учётом выявленных аспектов

Совокупность вышеперечисленных этапов является примером стандартного анализа разрывов (гар-анализа). Этот подход является стандартным для выявления необходимых изменений в правовом поле.

Результаты исследования

Проведенный в этом году анализ регуляторных аспектов внедрения ЦВЦБ в других странах не выявил существенных отличий от результатов исследований, отраженных в итоговом докладе 2021 года. Это объясняется тем фактом, что на данный момент количество ЦБ, внедривших цифровую валюту в качестве полноценного платёжного инструмента, не превышает 4 (Восточно-карибский центральный Банк, Центральный Банк Нигерии, Центральный банк Багамских островов и Банк Ямайки) [37].

В ходе анализа существующих НПА РК был выявлен ряд терминов, понятий и явлений, нуждающихся в законодательном закреплении для обеспечения необходимого правового статуса ЦТ.

ЦТ – это обязательство НБРК, эмитируемое в электронной форме и распространяемое в рамках двухуровневой финансовой архитектуры совместно с участниками рынка.

В целях законодательного закрепления понятия «цифровой тенге» предлагается внести соответствующие дополнения в Гражданский кодекс РК, Закон РК «О платежах и платёжных системах».

Оборот ЦТ включает эмиссию, размещение, хранение, передачу, продажу, покупку и погашение ЦТ.

В целях законодательного закрепления понятия «оборот цифрового тенге» предлагается внести соответствующие дополнения в Закон РК «О платежах и платёжных системах».

Субъекты, задействованные в обороте ЦТ – Национальный Банк РК, оператор ЦТ, банки второго уровня, физические лица и организации.

В целях законодательного закрепления прав, обязательств и ответственности субъектов, задействованных в обороте ЦТ, предлагается внести дополнения и изменения в Законы РК «О платежах и платёжных системах», «О Национальном Банке РК», «О банках и банковской деятельности в РК», «О персональных данных и их защите», «О стандартизации», «О валютном регулировании», «О реабилитации и банкротстве», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Кодекс РК «Об административных правонарушениях», Бюджетный кодекс РК, Уголовный кодекс РК, Предпринимательский кодекс РК, Налоговый кодекс РК. Возможны дополнительные изменения в других нормативно-правовых актах.

В конце раздела также представлена сводная таблица направлений и принципиальных отличий ЦТ от существующих концептов, закрепленных на законодательном уровне. Каждое из этих направлений и отличий нуждается в дальнейшей проработке в рамках работ по развитию платформы ЦТ и определения её легального статуса.

Отдельно также стоит отметить сложности, возникающие в процессе выработки механизмов регулирования ЦТ, обусловленные законотворческим процессом в рамках усовершенствования законодательства в области цифровых активов. В рамках рабочей группы заинтересованные лица высказывали различные точки зрения в отношении определения терминов, составных частей оборота цифровых активов, распределения функций между уполномоченными органами.

Более того, уполномоченный орган в области информатизации приступил к разработке Концепции Цифрового кодекса РК, что предполагает необходимость пересмотра в будущем тех выводов, к которым пришли в рамках настоящего исследования.

Направление	Концептуальные различия ЦТ
Определение ЦТ	<p>Безналичные денежные средства представляют собой обязательства кредитных организаций в качестве записей на банковских счетах/вкладах</p> <p>Наличные денежные средства представляют собой эмитированные денежные знаки НБРК</p> <p>ЦТ является обязательством НБРК, принципиально отличается от безналичных средств информационной средой, в которой формируются и используются ЦТ</p>
Обращение ЦТ	<p>Маркированные токены могут быть ограничены в обращении</p> <p>Будут определены новые роли участников рынка в зависимости от операционной модели ЦТ</p>
Технология	<p>Платформа ЦТ основана на гибридной технологии: комбинации децентрализованной и централизованной систем</p>
Новые стандарты	<p>Новая криптографическая библиотека платформы ЦТ</p> <p>Новые стандарты безопасности</p> <p>Новые стандарты данных при интеграции с другими системами</p> <p>Новые стандарты QR, NFC протокола, других каналов передачи данных о транзакциях</p>
Подделка и утрата данных ЦТ в рамках частного права	<p>Даже если данные ЦВЦБ на основе счета будут утеряны, например, в результате несчастного случая, гражданин имеет право требовать возвращения суммы на счет. По этой же причине пользователи могут требовать возврата ЦВЦБ</p> <p>Если данные ЦВЦБ на основе токенов будут утеряны, считается, что денежная стоимость исчезла. То есть пользователь не может претендовать на перевыпуск средств, хотя технически это реализуемо.</p> <p>Вопрос возможности восстановления средств в системе ЦТ остаётся открытым.</p> <p>Если в закон будут внесены изменения, чтобы включить подделку/дублирование ЦТ в состав преступлений, связанных с подделкой валюты, необходимо будет учесть особенности цифровой валюты (уровень сложности подделки/дублирования в больших масштабах в течение короткого времени)</p>

Направление

Концептуальные различия ЦТ

Обращение
взыскания на ЦТ
по частному праву

Обращение взыскания на ЦВЦБ, основанные на счетах, могут быть обработаны в соответствии с существующим процессом обращения взыскания на депозиты в частных банках, поскольку это аналогично требованиям по депозитам

Обращение взыскания на ЦВЦБ на основе токенов требует дальнейшего обсуждения.

Ограничения на
использование ЦТ
в соответствии с
антимонопольным
законодательст
вом

Согласно антимонопольному законодательству, НБРК как монопольный поставщик ЦТ обязан выполнять любые требования пользователей по проведению операций

Получение
информации в
соответствии с
нормативными
актами по ПОД/ФТ

В целях митигации рисков «цифрового бегства» могут быть различные уровни предоставления данных и проверки на требования ПОД/ФТ

Также в целях увеличения финансовой инклюзии могут быть предоставлен доступ к кошелькам ЦТ широкому населению с помощью упрощенных процессов проверки

Защита личной
информации

Система ЦТ предусматривает доступ к персональным данным пользователей со стороны БВУ/ВУ, но не со стороны НБРК.

Как и при существующей в РК платежной архитектуре, БВУ/ВУ имеет доступ к информации о индивидуальных операциях через ЦТ. Сюда входит информация об индивидуальных атрибутах (имя и дата рождения ФЛ); о платежах (сумма платежа и дата платежа); о коммерции (опционально; наименование приобретенных товаров/услуг и их цены за единицу).

Вопрос распределения ответственности между участниками системы и открытости/закрытости тех или иных данных в рамках платформы также нуждается в дальнейшей проработке

Выводы и оценки

Эффективность внедрения ЦТ и жизнеспособность его оборота непосредственно зависят от механизма правового регулирования ЦТ

Эффективность внедрения ЦТ и жизнеспособность его оборота непосредственно зависят от механизма правового регулирования ЦТ, четкого определения терминологии и составных частей оборота ЦТ в правовом поле.

Роли всех субъектов, задействованных в обороте ЦТ, их права, обязательства и ответственность должны быть распределены по логике их функционального назначения в жизненном цикле ЦТ без допущения дублирования функций, с четкими сроками, последовательностью действий и ответственностью за их нарушения.

Нормы об ответственности за нарушения в сфере оборота ЦТ должны быть адекватны последствиям таких нарушений, не только не допускать чрезмерную криминализацию сферы регулирования, но и быть достаточной сдерживающей превентивной мерой.

Внедрение ЦТ осуществляется на стыке нескольких регулируемых сфер

Внедрение ЦТ осуществляется на стыке нескольких регулируемых сфер, что влечет включение в ареал исследования, изменения и дополнения множества системообразующих и отраслевых правовых актов.

Далее требуется доработка операционной модели в регуляторной песочнице

Вышеописанный анализ позволил получить следующий вариант ответа: потенциально низкий уровень регуляторных издержек, далее требуется доработка операционной модели в регуляторной песочнице.

ИТОГОВАЯ ОЦЕНКА ДОРОЖНАЯ КАРТА

91-95
стр.

Итоговая оценка

На основании вышеизложенного, предварительно рекомендуется внедрить ЦТ. Вместе с тем, с учетом необходимости технологических доработок и проработки операционной модели рекомендуется обеспечить поэтапное внедрение за три года.

	Критерии	Предварительное заключение
1	Технологические преимущества	Реализуемы, требуется существенная доработка
2	Технологические риски	Контролируемы, требуется доработка (кибербезопасность, пропускная способность и т.д.)
3	Экономический эффект	Нейтральный
4	Экономические риски	Контролируемы, требуется выработка соответствующего регулирования
5	Готовность рынка	Достаточно высокая готовность на стороне внешних участников, задействованных в проекте
6	Оценка регуляторного воздействия	Потенциально низкий уровень регуляторных издержек, требуется доработка операционной модели
7	Выгоды и издержки для стейкхолдеров	Выгоды могут превосходить издержки в случае эффективной операционной модели

Дорожная карта

Реализация проекта ЦТ в 2022 году позволила определить ключевые параметры дизайна ЦТ, протестировать функционал на реальных пользователях, а также подтвердить технологическую реализуемость уникальных свойств ЦТ.

ПРЕДВАРИТЕЛЬНЫЙ ПОДХОД К ДОРОЖНОЙ КАРТЕ ВИДЕНИЕ ДО 2025 ГОДА

СТАДИЯ ПРОЕКТА



ОПИСАНИЕ



ВЫБОР ЦЕЛЕВОГО ТЕХНОЛОГИЧЕСКОГО РЕШЕНИЯ



Дорожная карта

Согласно Дорожной карте развития проекта в качестве основной задачи по развитию ЦТ является разработка платформы промышленного уровня (с подключением финансовых организаций, государственных организаций и других внешних участников) для запуска в опытную эксплуатацию.

Основными задачи по дальнейшему развитию платформы являются:

Разработка и тестирование расширенной функциональности ЦТ, включая:

- социальные выплаты от государственных органов населению (с использованием социального кошелька)
- государственные закупки
- новые сценарии программируемости ЦТ (включая смарт-контракты)
- обмен на другие формы денег
- восстановление, блокировка кошелька и др.

Исследование оптового ЦТ, проработка возможностей осуществления трансграничных платежей, а также тестирование трансграничных платежей с другими странами.

Разработка нефункциональных требований к целевой платформе (включая требования по информационной безопасности, производительности и др.).

Интеграция с:

- внешними участниками и платформами,
- национальными и международными платежными системами (в т.ч. для конвертации ЦТ в другие формы денег),
- национальными сервисами.

Проработка регуляторной и операционной моделей (включая проработку операционных аспектов функционирования ЦТ, макроэкономическое моделирование и проработка правовых аспектов внедрения ЦТ).

Вовлечение участников рынка в Digital Tenge Hub для совместного развития платформы ЦТ, создание технологической песочницы в R&D для разработки и тестирования собственных сценариев участников.

Определение решения «последней мили» (цифровые носители, карты и т.п.) и метода офлайн-платежей.

Подходы по развитию ЦВЦБ в других странах

Внедрение национальных цифровых валют в фокусе внимания центральных банков по всему миру. Согласно статистике CBDC Tracker, 91 центральный банк в мире исследует цифровые валюты, 29 центральных банков находятся в стадии пилотирования ЦВЦБ. Одной из ключевых тенденций в мире является исследование трансграничных платежей с использованием цифровых валют (проекты Jura, mBridge, Dunbar, Icebreaker и другие). Ниже представлены страны, которые существенно продвинулись в развитии розничных цифровых валют.

Проекты по развитию ЦВЦБ в других странах

Страна	Текущий статус	Ключевые особенности	Дальнейшее развитие
Китай [51-55]	<p>Оборот > 13 млрд \$ Провинции > 15 Физ. лица > 250 млн Мерчанты > 5 млн Количество транзакций > 360 млн</p> <p>Проект по трансграничным платежам (mBridge)</p>	<p>Один кошелек в одном банке (+дополнительные субкошельки)</p> <p>Подход к анонимности: анонимность на небольшие суммы и прослеживаемость больших сумм</p> <p>Офлайн-транзакции</p>	<p>Использование e-CNY в корпоративных расчетах, налогообложении и государственных платежах</p> <p>Запуск трансграничных платежей с Гонконгом</p> <p>Исследование трансграничных расчетов с BIS</p>
Швеция [56-58]	<p>Реализована вторая фаза проекта (с двумя внешними участниками)</p> <p>Третья фаза проекта в процессе реализации</p>	<p>Тестирование офлайн-функциональности</p> <p>Тестирование интеграции с POS-терминалами</p> <p>Различные модели хранения токенов</p> <p>Различные типы кошельков (в т.ч. анонимные на небольшие суммы)</p>	<p>Основные задачи третьей фазы проекта:</p> <p>Исследование программируемости денег</p> <p>Взаимодействие с внешними участниками</p> <p>Юридический статус e-krona</p> <p>Оценка и выбор технологического решения</p>
Россия [59, 60]	<p>В 2022 году осуществлялось тестирование прототипа платформы цифрового рубля (с вовлечением 15 коммерческих банков), разработка законодательства для внедрения</p>	<p>Доступ к кошельку через любую финансовую организацию, в которой обслуживается клиент</p> <p>Исследование офлайна</p> <p>Отсутствие анонимности</p>	<p>2023 год – пилотирование расчетов на реальных деньгах (С2В, В2С). Создание смарт-контрактов на платформе</p> <p>2024 год – поэтапное подключение к платформе всех кредитных организаций, платежи с участием государства (С2G, В2G, G2С, G2В), сотрудничество</p>

Страна	Текущий статус	Ключевые особенности	Дальнейшее развитие
Россия [59, 60]			<p>с другими ЦБ для осуществления трансграничных и валютно-обменных операций</p> <p>2025 год – реализация офлайн-режима, подключение небанковских финансовых посредников, финансовых платформ</p>
ЕС [61, 62]	<p>Этап исследования (2021-2023)</p> <p>Цель – проработка вопросов дизайна и модели распределения для конечных пользователей</p>	<p>Офлайн (в проработке, возможны лимиты на офлайн-кошельки)</p> <p>Контролируемая анонимность (отсутствие полностью анонимных кошельков)</p> <p>Лимиты на максимальную сумму ЦВЦБ на кошельке</p>	<p>Продолжение работ по дизайну ЦВЦБ, включая взаимодействие с финансовыми посредниками, проработка модели распределения, компенсации, ролевой модели</p> <p>Вовлечение стейкхолдеров в проект</p> <p>2023 год – решение о начале следующего этапа (этап разработки и тестирования технологического решения, бизнес-механизмов)</p>
США [63, 64]	<p>Выпущен указ Президента о криптовалютах и ЦВЦБ.</p> <p>Запущен пилотный проект с финансовыми компаниями в тестовой среде</p>	Офлайн (в проработке)	Реализация пилотного проекта, цель проекта – повысить скорость транзакций

СПИСОК ЛИТЕРАТУРЫ

97-100

стр.

Список литературы

Технология

1. Corda Documentation. URL: <https://docs.r3.com/en/platform/corda/4.6/open-source/node-database-tables.html>
2. ISO 20022 Financial Services - Universal financial industry message scheme
3. ISO/IEC 18004:2015 Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification
4. People's Bank of China (2021). Progress Progress Progress Progress of Research Research Research Research & Development Development Development Development of E-CNY in China <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>
5. Riksbank. (2022). E-krona pilot Phase 2 <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf>
6. The Korea Economic Daily. (2022). Bank of Korea to test CBDC on Samsung devices, not on iPhone <https://www.kedglobal.com/cryptocurrencies/newsView/ked202201250001>
7. Банк России. (2021). Концепция цифрового рубля. https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf
8. Модель принятия решений о внедрении Цифрового Тенге. (2022). <https://payfintech.kz/digital-tenge>
9. СТ РК 3712-2021. Код штриховой (QR-код), присваиваемый поставщиком платежных услуг или оператором платежной системы для осуществления платежей за предоставленные товары, работы или услуги в рамках предпринимательской деятельности

Экономика

10. Abilov, N. (2021). A Medium-Scale Bayesian DSGE Model for Kazakhstan with incomplete exchange rate pass-through. International Economic Journal, Vol. 35(4), pp. 486-522. <https://doi.org/10.1080/10168737.2021.1999298>
11. Abilov, N. and S. Rahardja. (2022). Optimal fiscal rules in a resource-rich economy. World Bank Policy Research Working Papers, Work in progress.
12. Abramova, S., Bohme, R., Elsinger, H., Stix, H. & Summer, M. (2022). What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents. Oesterreichische Nationalbank Working Paper, 241.
13. Agénor, P.R. (2016). Optimal fiscal management of commodity price shocks. Journal of Development Economics, Vol. 122(C), pp. 183-196. <https://doi.org/10.1016/j.jdeveco.2016.05.005>
14. Assenmacher, K., A. Berentsen, C. Brand and N. Lamersdorf. (2021). A unified framework for CBDC design: remuneration, collateral haircuts and quantity constraints. ECB Working Papers, No. 2578.

15. Bachetta, P. and E. Perazzi. (2021). CBDC as imperfect substitute for bank deposits: A macroeconomic perspective. Swiss Finance Institute Research Paper, No. 21-81.
16. Barrdear, J. and M. Kumhof. (2021). The macroeconomics of central bank digital currencies. *Journal of Economic Dynamics and Control*, Vol. 142, pp. 104148. <https://doi.org/10.1016/j.jedc.2021.104148>.
17. Bijlsma, M., Cruijssen, C., Jonker, N. & Reijerink, J. (2021). What triggers consumer adoption of CBDC? De Nederlandsche Bank Working Paper
18. Brunnermeier, M.K. and D. Niepelt. (2019). On the equivalence of private and public money. *Journal of Monetary Economics*, 106(C):pp. 27-41.
19. Burlon, L. C. Montes-Galdón, M.A. Muñoz and F. Smets. (2022). The optimal quantity of CBDC in a bank-based economy. ECB Working Paper Series, No. 2689.
20. Chiu, J., M. Davoodalhosseini, J. H. Jiang, and Y. Zhu. (2019). Central bank digital currency and banking. Bank of Canada Staff Working Papers, No. 19-20.
21. George, A., T. Xie, and J. Alba. (2018). Central bank digital currency with adjustable interest rate in small open economies. Mimeo.
22. Gerali, A., S. Neri, L. Sessa and F.M. Signoretti. (2010). Credit and Banking in a DSGE Model of the Euro Area. *Journal of Development Economics*, Vol. 42(s1), pp. 107-141. <https://doi.org/10.1111/j.1538-4616.2010.00331.x>
23. Huynh, K., Molnar, J., Shcherbakov, O. & Yu, Q. (2020). Demand for payment services and consumer welfare: the Introduction of a central bank digital currency. Bank of Canada working papers.
24. Kantar Public. (2022). Study on new digital payment methods. Kantar Public- commissioned by the European Central Bank
25. Kim, Y.S. and O. Kwon (2019) Central Bank Digital Currency and Financial Stability. Bank of Korea Working Paper No. 2019-6. http://papers.bok.or.kr/RePEc_attach/wpaper/english/wp-2019-6.pdfhttp://papers.bok.or.kr/RePEc_attach/wpaper/english/wp-2019-6.pdf
26. Konebayev, E. (2020). Estimation of a Small Open Economy DSGE Model for Kazakhstan. NAC Analytica Working Paper, No. 6.
27. Kumhof, M. and C. Noone. (2021) Central bank digital currencies - design principles for financial stability. *Economic Analysis and Policy*, Vol. 71, pp. 553-572. <https://doi.org/10.1016/j.eap.2021.06.012>[doi: 10.1016/j.eap.2021.06.012](https://doi.org/10.1016/j.eap.2021.06.012).
28. Li, J. (2021). Predicting the Demand for Central Bank Digital Currency: A Structural Analysis with Survey Data. Conditionally accepted by *Journal of Monetary Economics*.
29. Minesso, M.F., A. Mehl and L. Stracca. (2022). Central bank digital currency in an open economy. *Journal of Monetary Economics*, Vol. 127, pp. 54-68. <https://doi.org/10.1016/j.jmoneco.2022.02.001>[doi: 10.1016/j.jmoneco.2022.02.001](https://doi.org/10.1016/j.jmoneco.2022.02.001)

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

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

Экосистема

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

Операционная модель

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

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

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

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

Регулирование

37. Atlantic Council's CBDC tracker

38. Гражданский Кодекс РК

39. КоАП РК

40. Бюджетный Кодекс РК

41. Уголовный Кодекс РК

42. Предпринимательский Кодекс РК

43. Закон РК «О платежах и платежных системах»

44. Закон «О Национальном Банке РК»

45. Закон «О банках и банковской деятельности в РК»

46. Закон «О персональных данных и их защите»

47. Закон «О стандартизации»

48. Закон «О валютном регулировании»

49. Закон «О реабилитации и банкротстве»

50. Закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

Дорожная карта: обзор стран

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

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

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

54. Bank of China: Digital yuan transactions volume crossed \$14B mark [Bank of China: Digital yuan transactions volume crossed \\$14B mark \(cointelegraph.com\)](https://www.cointelegraph.com/news/bank-of-china-digital-yuan-transactions-volume-crossed-14-billion-mark)

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

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

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

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

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

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

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

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

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

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

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

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

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

ПРИЛОЖЕНИЯ

102-145

стр.

Приложение 1

Сценарий

Технологические особенности

Открытие кошельков

Кошельки структурных участников (БВУ/ВУ/ гос. учреждения) формируются при развертывании и подключении нод к сети.

Процесс открытия кошельков клиентов (ФЛ, ТСП) основывается на создании клиентами на уровне своих устройств пар ключей (приватный, публичный) и регистрации части из них на ноде участника (БВУ/ВУ). Владение ключами позволяет клиенту полностью управлять операциями с ЦТ (часть приватного ключа, которая позволяет проводить операции, есть только у клиента). Протестировано три модели кошельков.

Эмиссия и распределение БВУ/ВУ и ГУ

Эмиссия токенов – уникальная транзакция, доступная только НБРК, что обеспечивает надежность жизненного цикла ЦТ. Ограничения по возможности совершения эмиссии достигаются с помощью ролевой модели. Во всех транзакциях для скрытия сумм использовалось обязательство Педерсена (Pedersen Commitment), позволяющее скрыть суммы в транзакции, а также подпись (Kernel signature), удостоверяющая формирование обязательств и доказывающая, что скрытие сумм произведено корректно. Особенность транзакции эмиссии заключается в отсутствии input токена.

Распределение ЦТ ФЛ

Так как кошелек клиента и БВУ/ВУ связаны с одним БВУ/ВУ, транзакция происходит с участием одной ноды БВУ/ВУ и ноды нотариуса. Создаются транзакции, где получатели - ФЛ, представленные нодой обслуживающих БВУ/ВУ. В ходе любых транзакций с токенами (перевод, покупка, распределение) задействуется механизм подбора минимальных токенов для формирования суммы транзакции.

Маркировка токенов

Возможные типы специальных токенов с различными видами ограничений определены заранее (виды ограничений: по времени, по количеству, по получателю ЦТ). Реестр типов токенов и их ограничений хранится на нодах участников. Условия расходования специальных токенов запрашиваются клиентом вместе с запросом баланса.

Распределение специальных ЦТ ФЛ

Механизм распределения специальных токенов отличается от распределения стандартных ЦТ тем, что в нем участвует две ноды – нода государственного учреждения и нода БВУ/ВУ.

С2С-переводы (по QR-коду)

Как способ передачи реквизитов или деталей платежа от одного участникам транзакции другому используется QR-код.

Если отправитель выбрал опцию скрытия данных, при переводе будут использованы скрытые значения (stealth).

Перед отправкой запроса инициации транзакции в ноду клиента, на стороне клиента происходит подписание транзакции с помощью приватного ключа.

С2С-переводы (по номеру телефона)

Для перевода по номеру телефона происходит запрос в реестр алиасов (ID Center), чтобы получить адрес кошелька клиента и наименования банка, обслуживающего кошелек. Скрытие данных и подписание транзакции происходит аналогично сценарию перевода С2С по QR.

Сценарий

Технологические особенности

Покупка

(стандартные ЦТ)

Передача данных о получателе происходит с помощью QR-кода от продавца клиенту. Скрытие данных и подписание транзакции происходит аналогично сценарию перевода С2С (по QR).

Покупка

(специальные ЦТ)

Передача данных о получателе происходит с помощью QR-кода от продавца клиенту. Скрытие данных и подписание транзакции происходит аналогично сценарию перевода С2С (по QR). На уровне ноды осуществляется проверка корректности выполнения условий, заложенных в тот или иной вид специальных ЦТ.

Перевыпуск

(вкл. техническое погашение)

Перевыпуск осуществляется автоматически (без прямого участия клиента) в 4 последовательных транзакции (эмиссия, распределение, перевод, погашение).

Мониторинг

- Для отслеживания показателей MVP пилотной платформы реализован сбор и обработка по направлениям:
- Мониторинг нефункциональных параметров при проведении транзакций.
- Мониторинг инфраструктурных параметров MVP пилотной платформы.
- Дополнительно организована витрина данных для построения бизнес-аналитики.

Офлайн-платежи (с цепочкой офлайн-транзакций)

Во время проведения офлайн-транзакции устройства пользователей должны находиться в пределах радиуса действия NFC-соединения. При проведении офлайн транзакций на устройствах клиентов сохраняются платежные поручения. В момент выхода любого из участников транзакции в онлайн происходит отправка всех платежных поручений с устройства участника транзакции (ФЛ и/или ТСП) на ноду БВУ/ВУ участника транзакции и синхронизация ЦТ на устройстве и в хранилище ноды БВУ/ВУ.

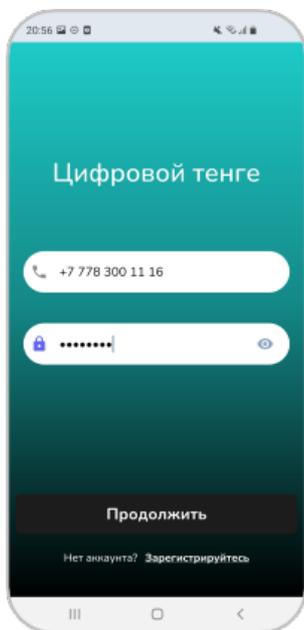
В случае, когда второй участник транзакции выходит в онлайн, одно и то же неподтвержденное платежное поручение отправляется на платформу ЦТ второй раз, но проведение транзакции на платформе ЦТ происходит только для первого платежного поручения. Во второй раз оно уже считается обработанным и игнорируется. Таким образом, гарантируется отсутствие многократного использования токенов.

ФЛ MVP

Открытие и пополнение кошелька

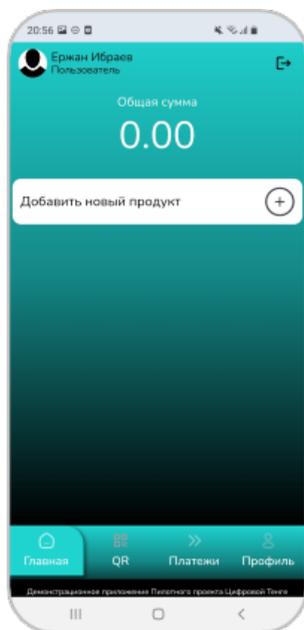
01

ФЛ регистрируется и авторизуется в приложении



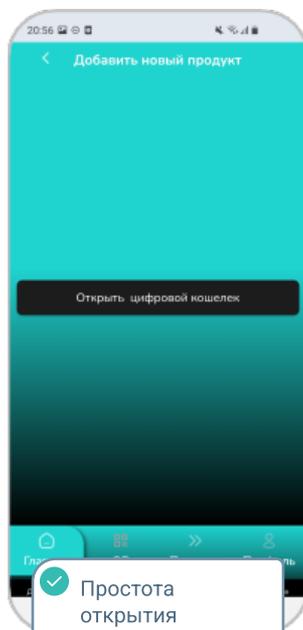
02

ФЛ выбирает «Добавить новый продукт»



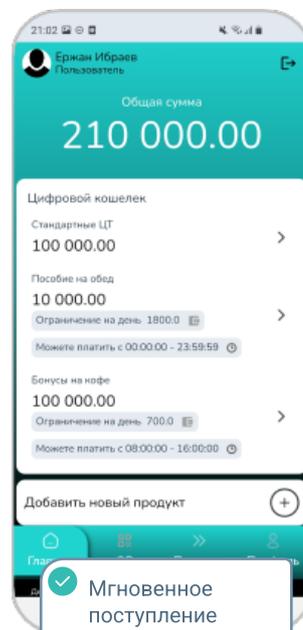
03

ФЛ открывает цифровой кошелек



04

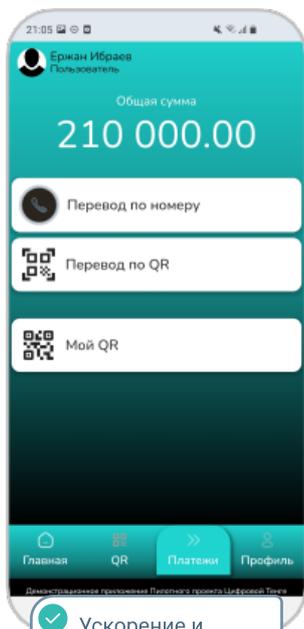
ФЛ видит зачисление ЦТ на кошелек



Переводы

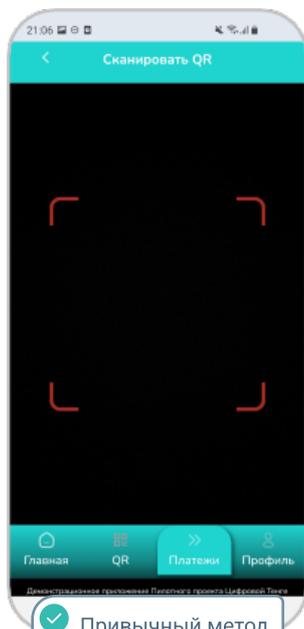
05

ФЛ переходит в раздел «Платежи» для перевода ЦТ другому ФЛ



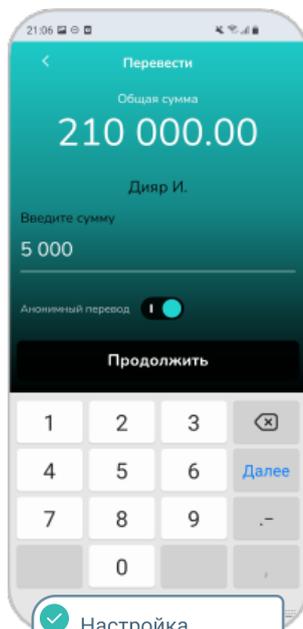
06

ФЛ выбирает «Перевод по QR», сканирует QR другого ФЛ



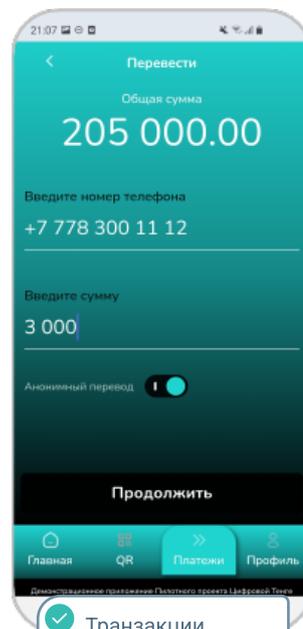
07

ФЛ вводит сумму перевода, подтверждает транзакцию



08

ФЛ выбирает «Перевод по номеру», вводит номер телефона и сумму, подтверждает транзакцию

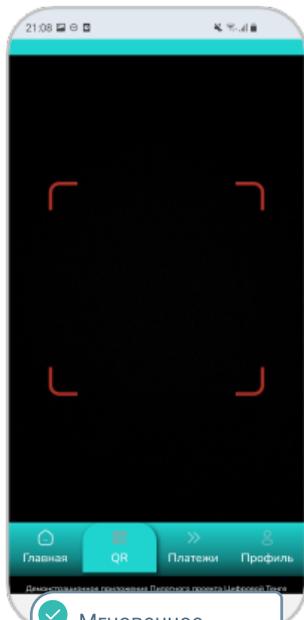


ФЛ MVP

Покупка

09

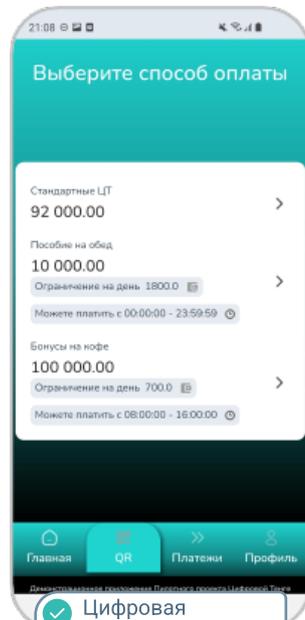
ФЛ переходит в раздел «QR» для совершения покупки, сканирует QR ТСП



✓ Мгновенное поступление средств

10

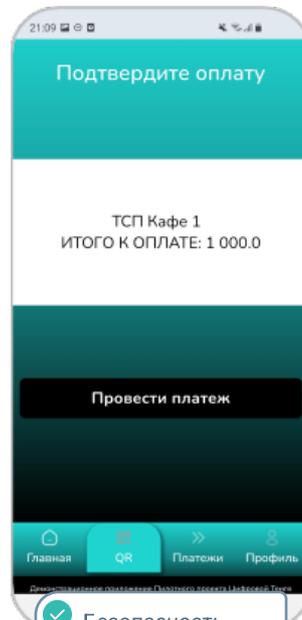
ФЛ выбирает тип ЦТ для оплаты покупки



✓ Цифровая альтернатива наличным денежным средствам

11

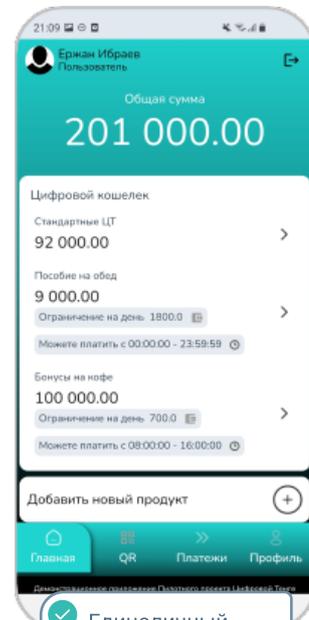
ФЛ проверяет данные и подтверждает транзакцию



✓ Безопасность транзакций

12

ФЛ видит обновленный баланс на цифровом кошельке



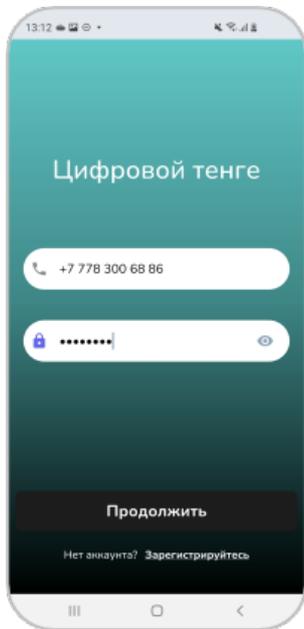
✓ Едиличный контроль над средствами

ТСП MVP

Открытие и кошелек

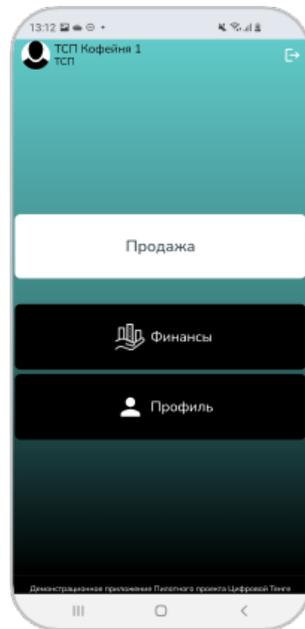
01

ТСП регистрируется и авторизуется в приложении



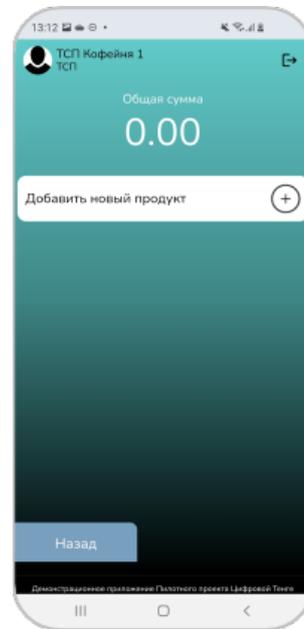
02

ТСП переходит в раздел «Финансы»



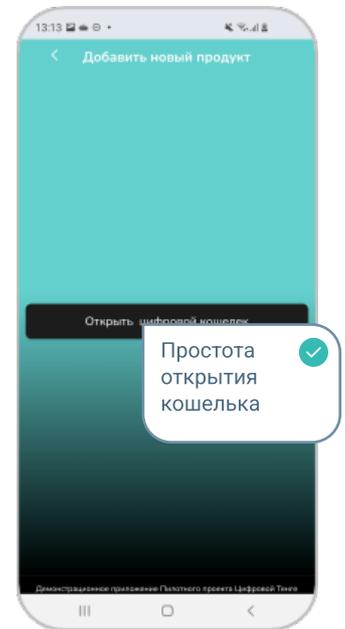
03

ТСП выбирает «Добавить новый продукт»



04

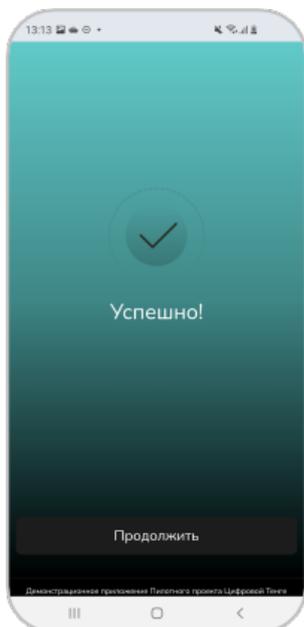
ТСП открывает цифровой кошелек



Продажа

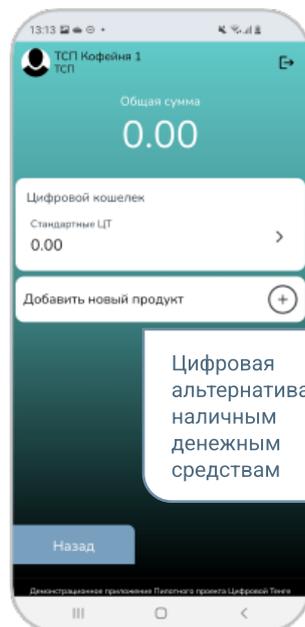
05

ТСП получает уведомление об успешном открытии цифрового кошелька



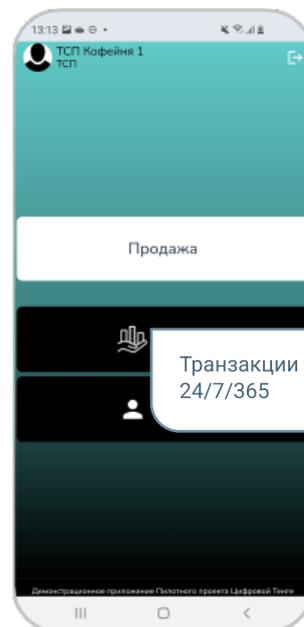
06

ТСП видит баланс цифрового кошелька



07

ТСП переходит в раздел меню «Продажа»



08

ТСП вводит сумму покупки (за стандартные или специальные ЦТ)

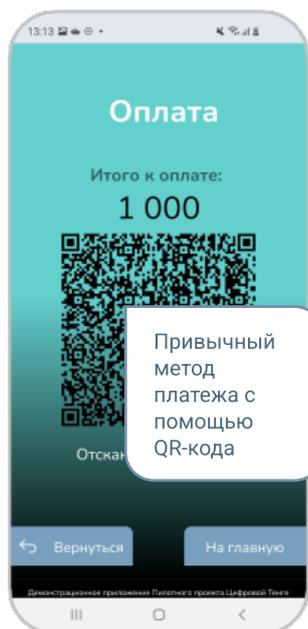


ТСП MVP

Продажа и проверка истории транзакций

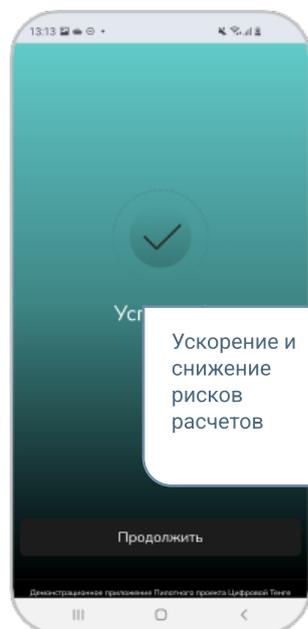
09

Происходит генерация QR-кода



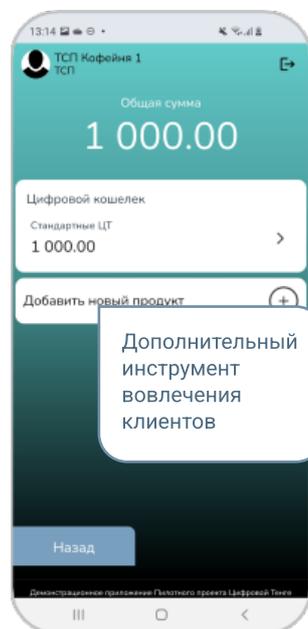
10

ТСП получает уведомление об успешном завершении транзакции



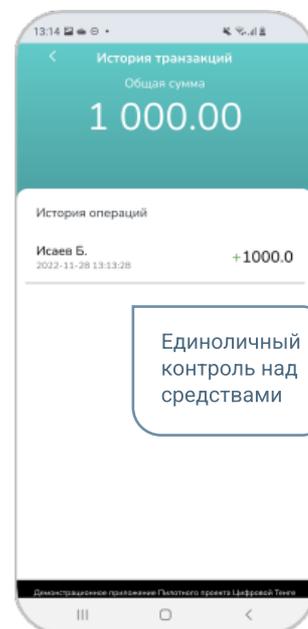
11

ТСП видит обновленный баланс на цифровом кошельке



12

ТСП проверяет историю транзакций



Открытие и пополнение кошелька

01

ФЛ авторизуется в приложении



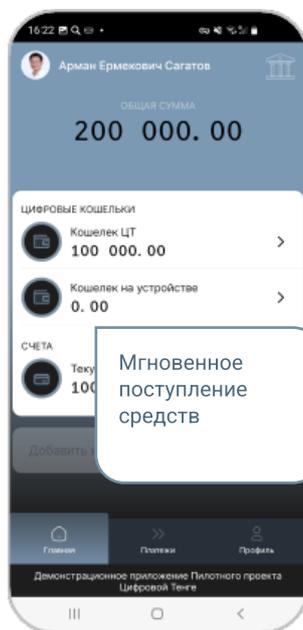
02

ФЛ открывает цифровые кошельки (онлайн и офлайн)



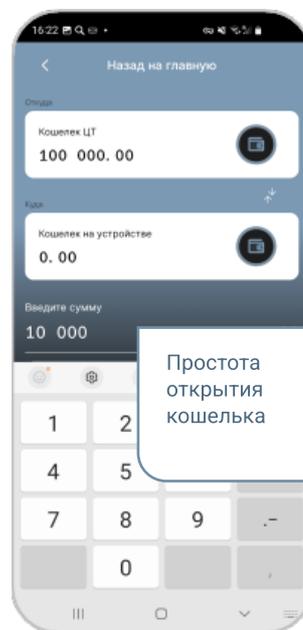
03

ФЛ видит зачисление ЦТ на онлайн-кошелек



04

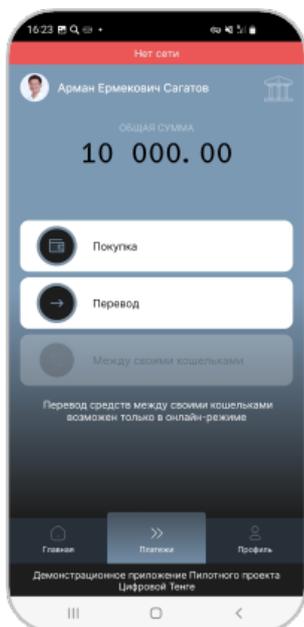
ФЛ переходит в раздел «Платежи» для перевода ЦТ на офлайн-кошелек



Перевод в офлайне

05

ФЛ переводит устройство в офлайн-режим, переходит в раздел «Платежи» и выбирает «Перевод»



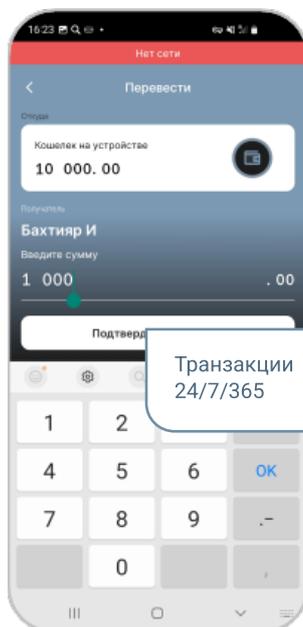
06

ФЛ указывает, что будет отправителем ЦТ в транзакции и сканирует QR-код получателя ЦТ



07

ФЛ вводит сумму перевода, подтверждает транзакцию



08

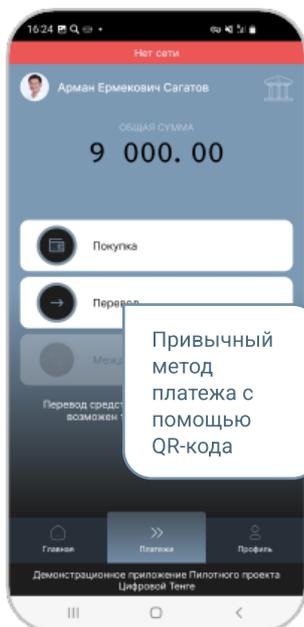
ФЛ подносит устройство к устройству другого ФЛ для осуществления перевода (NFC-перевод)



Покупка в офлайне, синхронизация

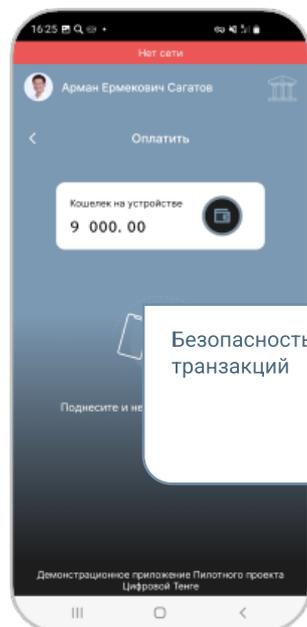
09

ФЛ переходит в раздел «Платежи» и выбирает «Покупка»



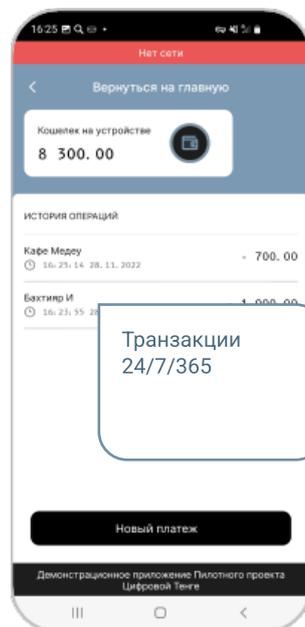
10

ФЛ подносит устройство к устройству ТСП для осуществления покупки



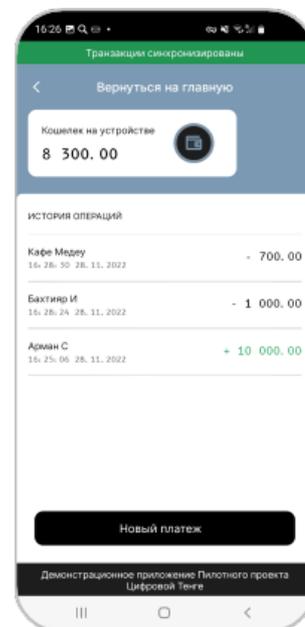
11

ФЛ проверяет историю транзакций в офлайн-режиме



12

ФЛ подключается к Интернету, происходит синхронизация транзакций

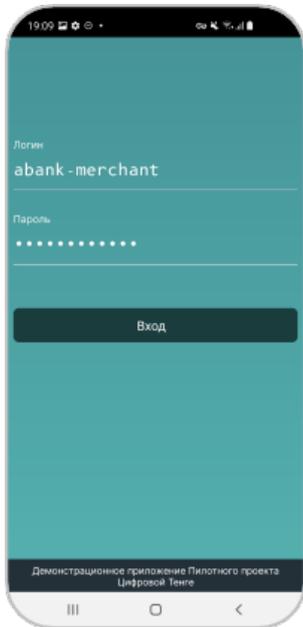


ТСП R&D

Открытие и кошелек

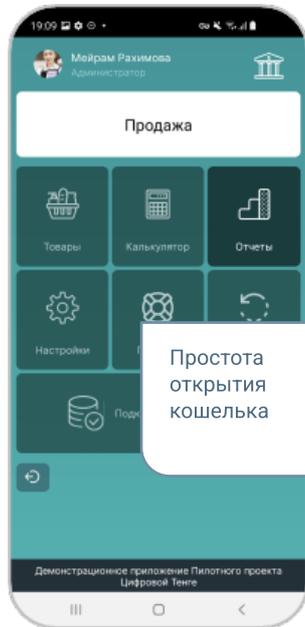
01

ТСП авторизуется в приложении



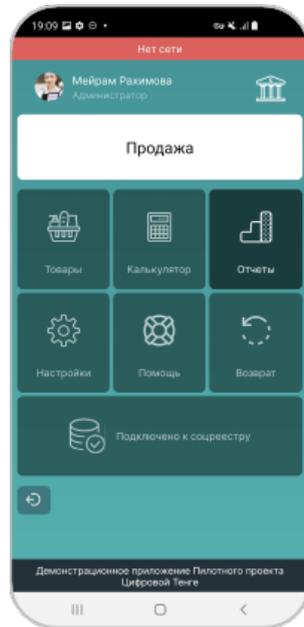
02

Кошельки открываются автоматически, ТСП видит главное меню



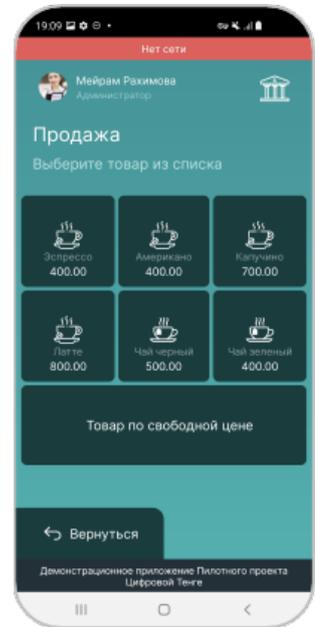
03

ТСП переводит устройство в офлайн-режим



04

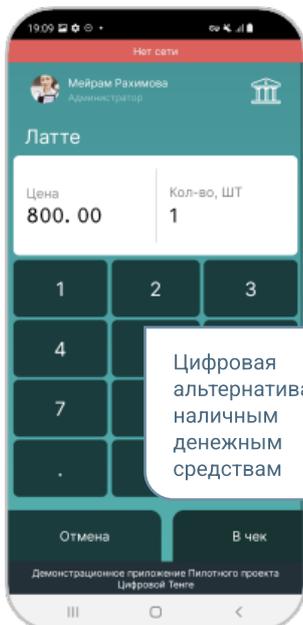
ТСП переходит в раздел «Продажа»



Открытие кошелька и покупка

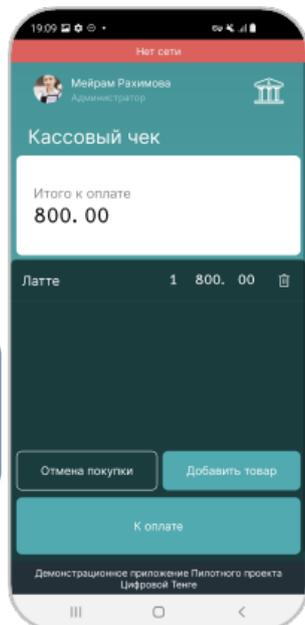
05

ТСП выбирает товар для продажи или вводит сумму ЦТ к оплате



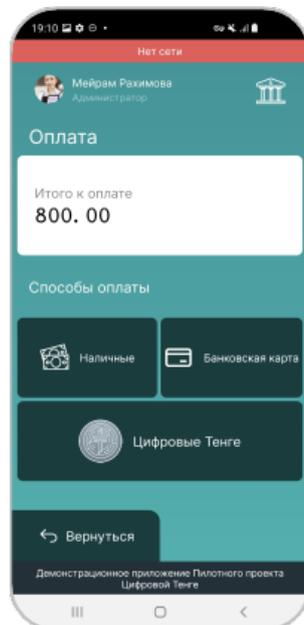
06

ТСП нажимает «К оплате»



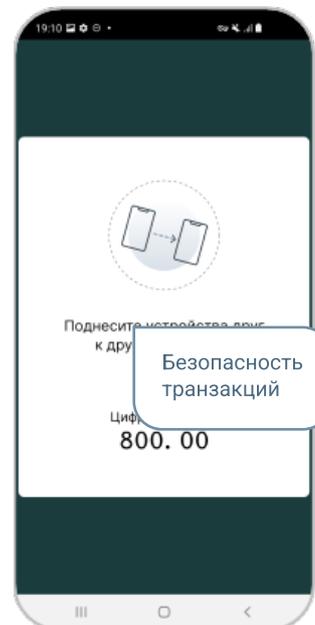
07

ТСП выбирает «Цифровые Тенге» в качестве способа оплаты



08

ТСП подносит устройство к устройству ФЛ для проведения транзакции покупки



Покупка и проверка истории транзакций

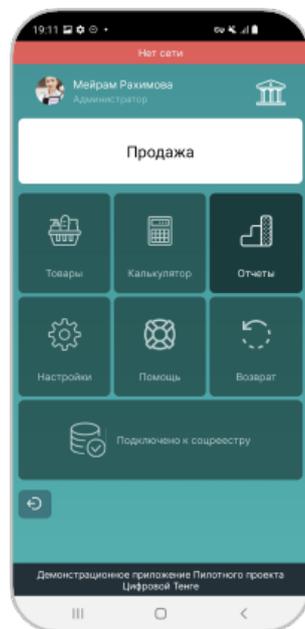
09

ТСП получает уведомление об успешном завершении транзакции



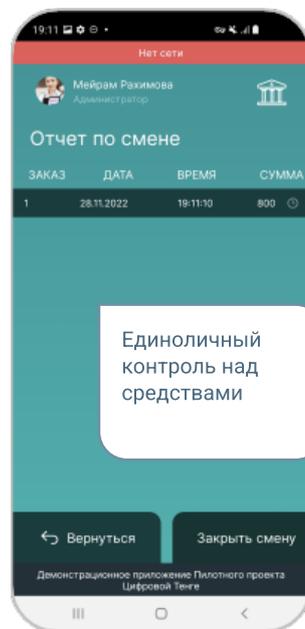
10

ТСП переходит в меню, в раздел «Отчеты»



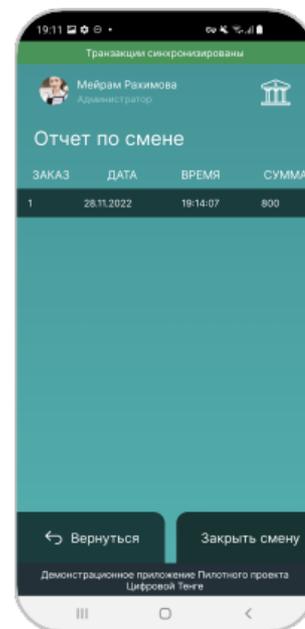
11

ТСП проверяет историю транзакций в офлайн-режиме



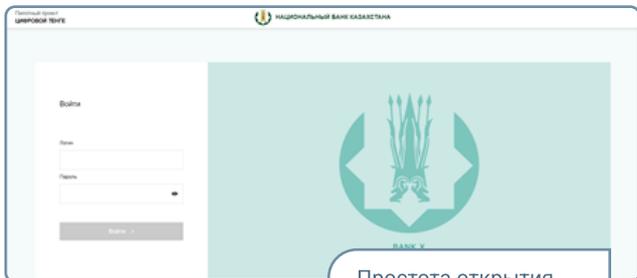
12

ТСП подключается к Интернету, происходит синхронизация транзакций



ОТКРЫТИЕ И ПОПОЛНЕНИЕ КОШЕЛЬКА 01

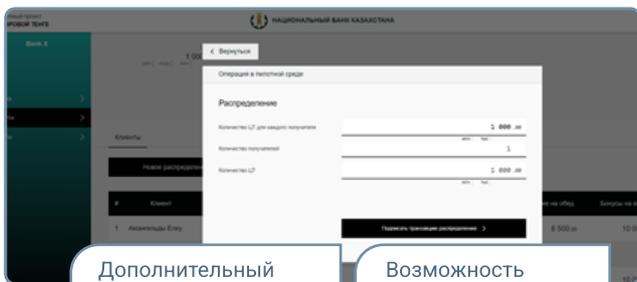
БВУ/ВУ получает доступ к порталу и открывает цифровой кошелек



Простота открытия кошелька

ОБСЛУЖИВАНИЕ КОШЕЛЬКОВ ФЛ 03

БВУ/ВУ осуществляет обслуживание кошельков пользователей, распределение ЦТ пользователям и проверку транзакций

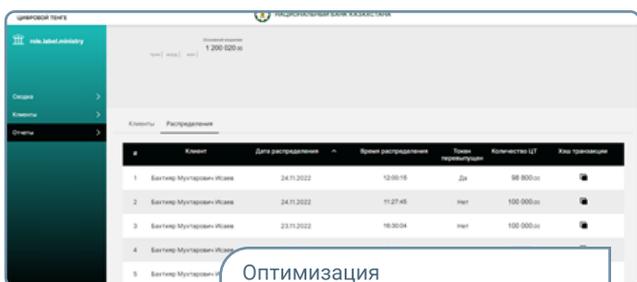


Дополнительный инструмент вовлечения клиентов

Возможность предоставления новых сервисов

ПЕРЕВЫПУСК 05

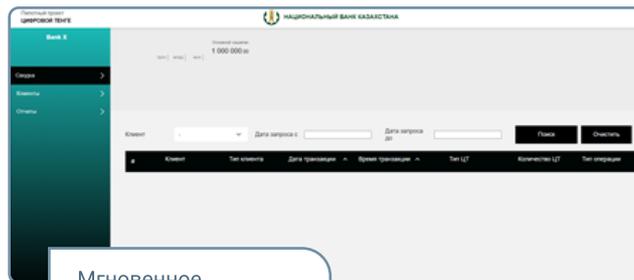
БВУ/ВУ осуществляет запрос перевыпуска ЦТ: погашение токена с длинной историей и эмиссия нового токена



Оптимизация производительности (времени проведения транзакции)

02 ОТКРЫТИЕ И ПОПОЛНЕНИЕ КОШЕЛЬКА

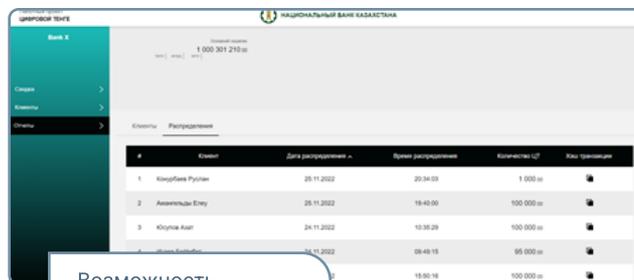
БВУ/ВУ видит зачисление ЦТ на кошелек (перевод из других форм денежных средств / обмен на резервы будет реализован на следующем этапе проекта)



Мгновенное поступление средств

04 МОНИТОРИНГ

БВУ/ВУ осуществляет мониторинг использования ЦТ клиентами



Возможность отслеживаемости ЦТ

ОТКРЫТИЕ И ПОПОЛНЕНИЕ КОШЕЛЬКА 01

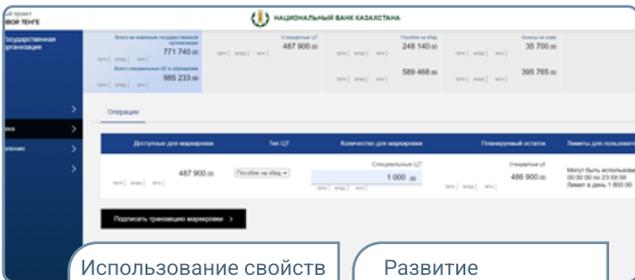
ГУ получает доступ к порталу и открывает цифровой кошелек



Простота открытия кошелька

МАРКИРОВКА ЦТ 03

БВУ/ВУ осуществляет обслуживание кошельков пользователей, распределение ЦТ пользователям и проверку транзакций

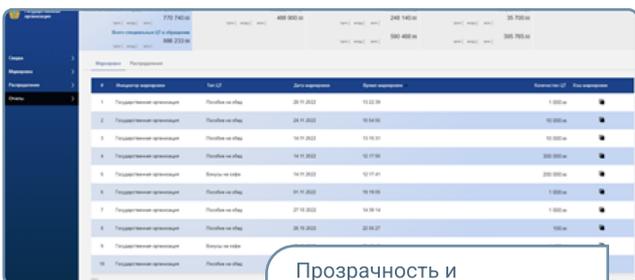


Использование свойств программируемости ЦТ

Развитие инновационности финансового сектора

МОНИТОРИНГ 05

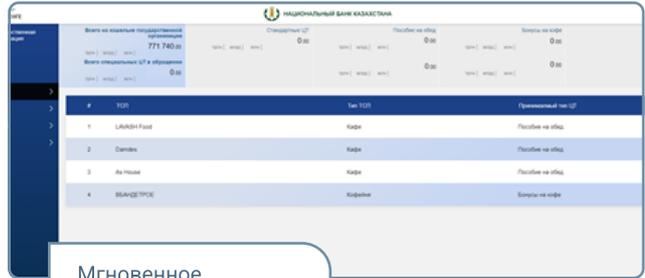
ГУ осуществляет мониторинг специальных ЦТ (отслеживает целевое использование)



Прозрачность и отслеживаемость социальных выплат

02 ОТКРЫТИЕ И ПОПОЛНЕНИЕ КОШЕЛЬКА

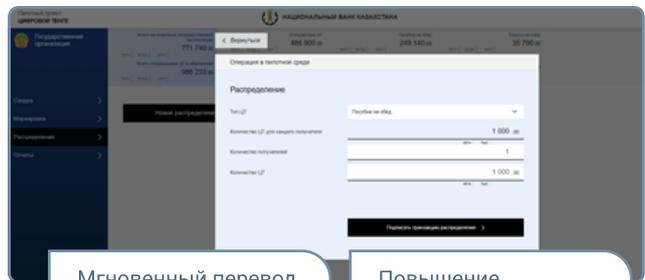
ГУ видит зачисление ЦТ на кошелек (перевод из других форм денежных средств / обмен на резервы будет реализован на следующем этапе проекта)



Мгновенное поступление средств

04 РАСПРЕДЕЛЕНИЕ СПЕЦИАЛЬНЫХ ЦТ

ГУ распределяет специальные ЦТ физическим лицам

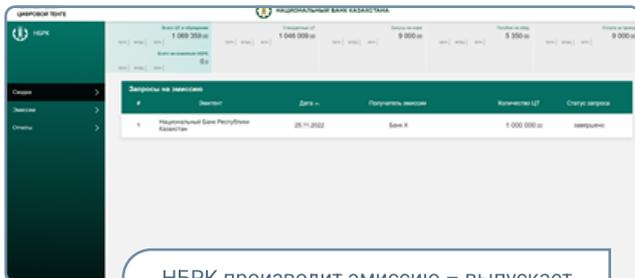


Мгновенный перевод средств (без посредников)

Повышение эффективности социальных выплат и инклюзивности

ЭМИССИЯ И РАСПРЕДЕЛЕНИЕ СРЕДСТВ 01

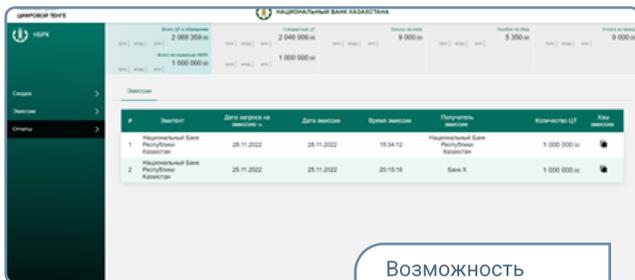
НБРК производит эмиссию ЦТ и их распределение



НБРК производит эмиссию – выпускает в оборот новые ЦТ. Осуществляется распределение выбранных ЦТ на кошельки участников 2 уровня – ГУ и БВУ/ВУ (перевод из других форм денежных средств / обмен на резервы будет реализован на следующем этапе проекта)

МОНИТОРИНГ 03

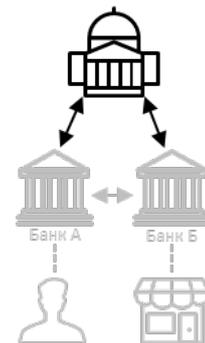
НБРК осуществляет мониторинг выпущенных ЦТ



Возможность отслеживаемости ЦТ

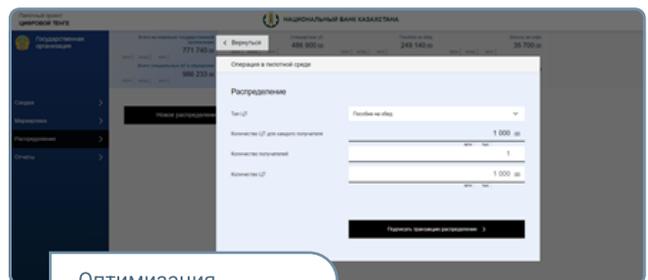
02 ВЗАИМОДЕЙСТВИЕ С КЛИЕНТАМИ ФЛ И ТСП

НБРК проверяет уникальность токена, участвующего в транзакции



04 ПЕРЕВЫПУСК

НБРК осуществляет перевыпуск ЦТ: погашение токена с длинной историей и эмиссия нового токена без истории

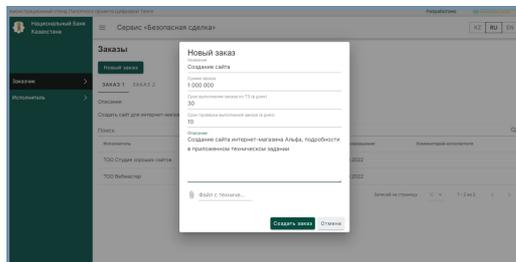


Оптимизация производительности (времени проведения транзакции)

Сценарий «Безопасная сделка»

СОЗДАНИЕ ЗАКАЗА 01

Исполнитель создаёт заказ, указывая сумму и сроки выполнения. В момент создания заказа происходит проверка наличия указанной суммы в кошельке ЦТ заказчика и создаётся смарт-контракт

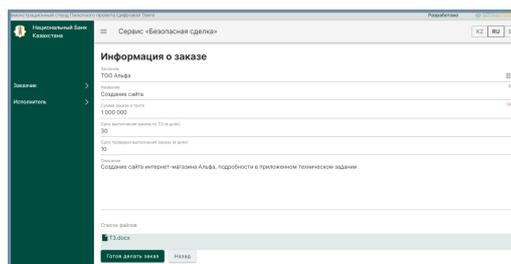
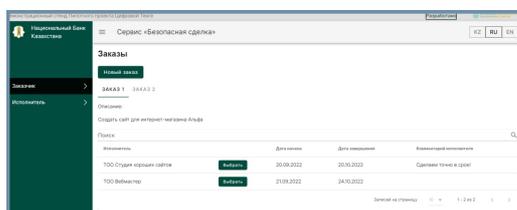


02 ЗАЯВКА НА ВЫПОЛНЕНИЕ ЗАКАЗА

Потенциальные исполнители видят список заказов, могут просмотреть подробности заказа и предложить свои услуги

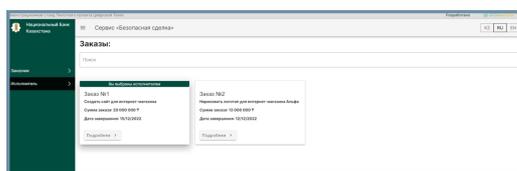
ЗАКАЗЧИК ВЫБИРАЕТ ИСПОЛНИТЕЛЯ 03

Заказчик выбирает среди откликнувшихся исполнителей. После того, как исполнитель будет выбран, ЦТ на кошелек заказчика будут зарезервированы на срок выполнения заказа. Исполнитель узнаёт об этом и приступает к выполнению заказа безопасной сделки



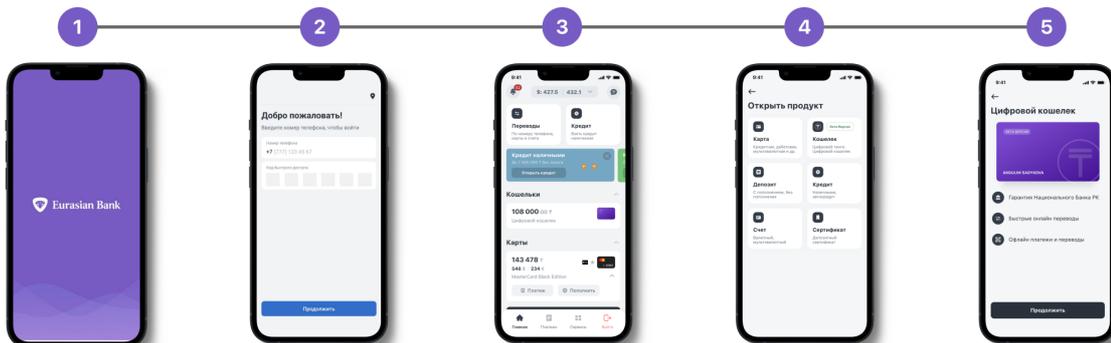
ЗАКАЗЧИК ВЫБИРАЕТ ИСПОЛНИТЕЛЯ 04

Исполнитель выполняет заказ и получает оплату. После выполнения заказа исполнитель сообщает об этом заказчику. Заказчик подтверждает выполнение и средства переходят на кошелек ЦТ исполнителя. Каждый этап сделки фиксируется в смарт-контракте

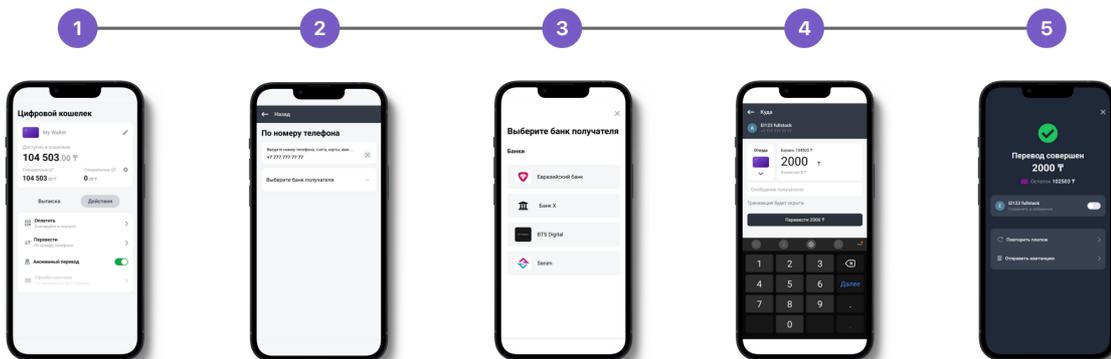


Сценарии Евразийского банка

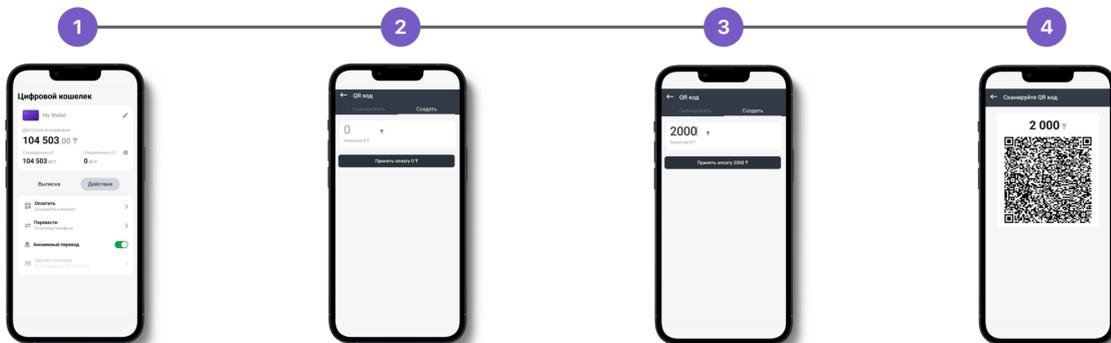
Открытие Цифровой кошелька



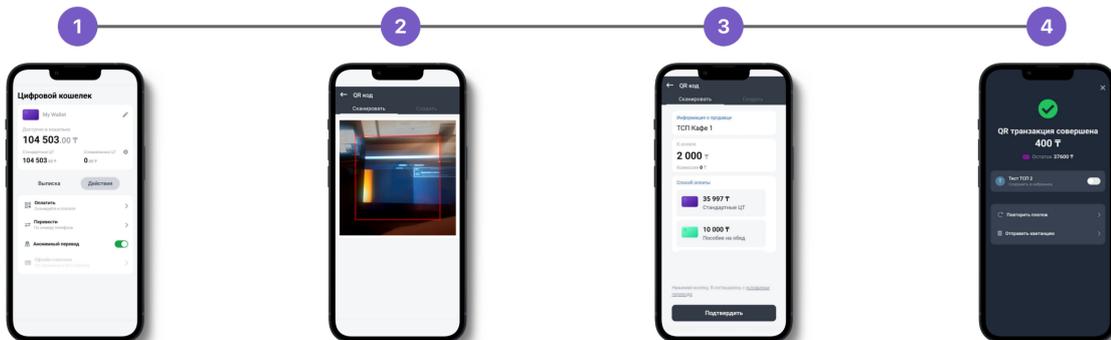
Оплата по номеру телефона



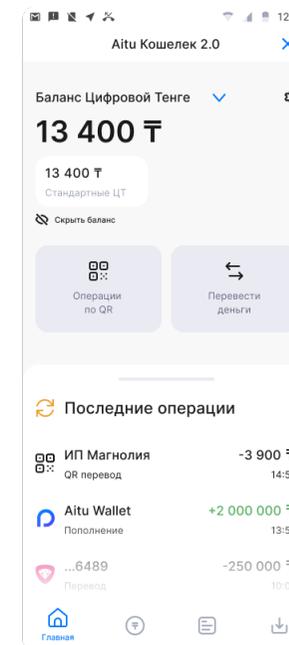
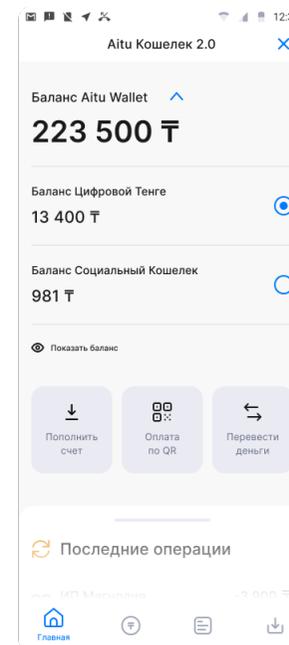
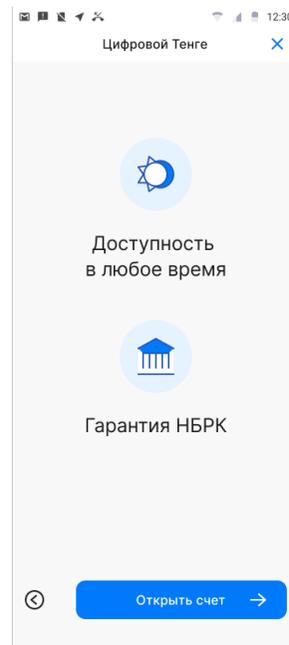
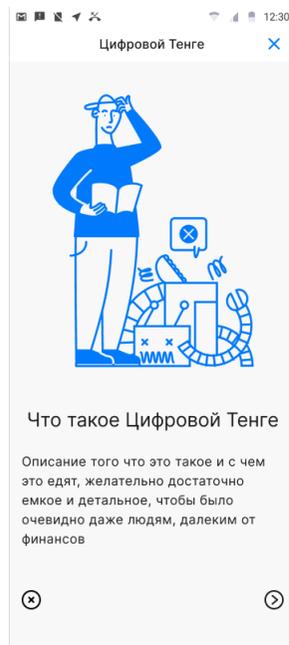
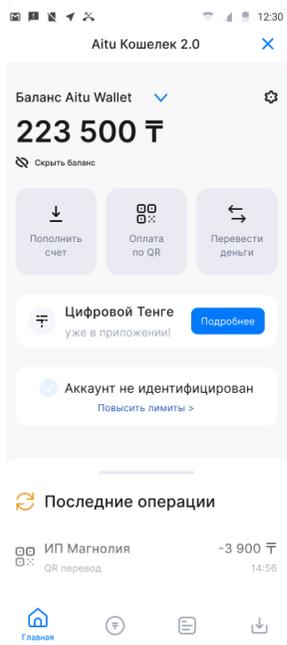
Принятие по QR-коду



Сканирование оплаты по QR-коду



Сценарии BTS Digital



1

Пользователь авторизуется в Aitu Wallet, нажимает на "Подробнее" о Цифровом Тенге

2

Пользователь знакомится с краткой информацией о ЦТ

3

Пользователь нажимает на "Открыть счет"

4

Пользователь видит сообщение о том, что кошелек создан и нажимает "На главный экран"

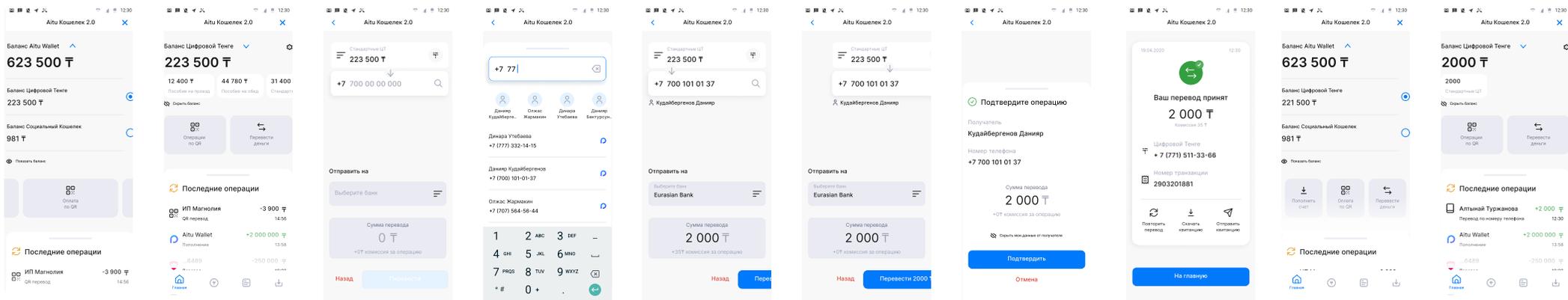
5

Пользователь видит на главной странице баланс цифрового тенге. Нажимает на него.

6

Пользователь видит детали Цифрового кошелька: виды ЦТ и активные кнопки: оплатить, перевести, история транзакций

Сценарии BTS Digital



Пользователь 1 выбирает баланс Цифрового Тенге

Пользователь 1 нажимает на "Перевести деньги"

Пользователь 1 вбивает все необходимые данные для перевода

У пользователя есть возможность быстрого дополнения номера из списка контактов

Пользователь выбирает банк

Пользователь-1 вводит количество ЦТ для перевода Пользователю-2

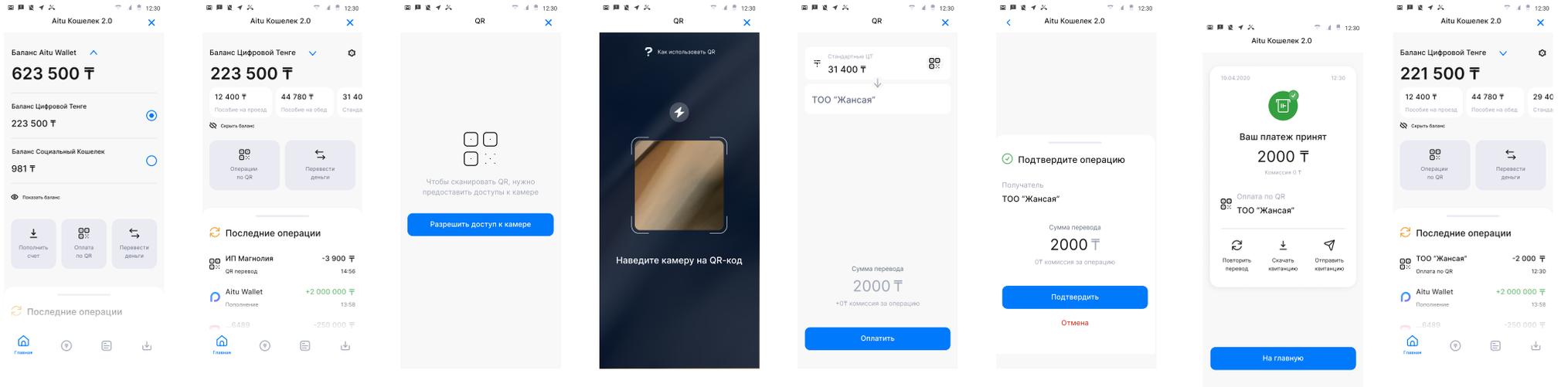
Пользователь-1 подтверждает данные по переводу

Пользователь-1 видит, что операция прошла успешно. Появилась возможность вернуться на главную страницу

Пользователь видит обновленный баланс цифрового тенге в Aitu Wallet

Пользователь-2 видит обновленное количество ЦТ. Данные о переводе можно проверить в истории транзакций.

Сценарии BTS Digital



1

Пользователь авторизуется в приложении Aitu Wallet

2

Пользователь выбирает баланс Цифрового Тенге, нажимает "Операции по QR"

3

Пользователь дает согласие на использование камеры телефона

4

Пользователь сканирует QR с устройства кассира

5

Пользователь выбирает способ оплаты стандартными ЦТ. Получатель и сумма платежа известны и статичны, нажимает на "Оплатить".

6

Пользователь подтверждает данные по платежу

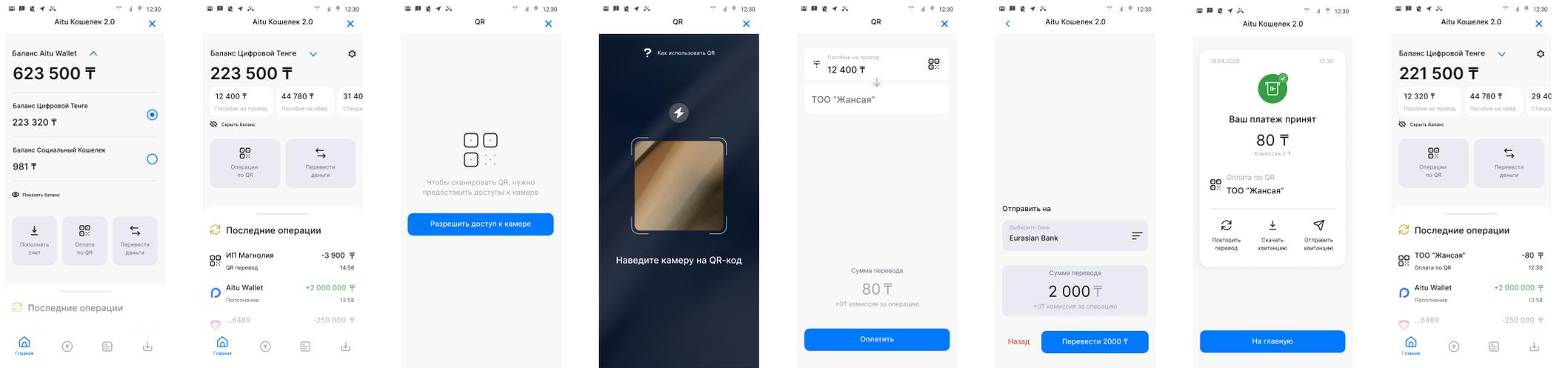
7

Пользователь видит подтверждение платежа и выходит на главную страницу

8

Пользователь видит обновленный баланс цифрового тенге в Aitu Wallet

Сценарии BTS Digital



1

Пользователь авторизуется в приложении Aitu Wallet

2

Пользователь выбирает баланс Цифрового Тенге, нажимает "Операции по QR"

3

Пользователь дает согласие на использование камеры телефона

4

Пользователь считывает QR с устройства для оплаты картой в автобусе

5

Пользователь выбирает способ оплаты специальными ЦТ: Пособие на проезд. Получатель и сумма платежа известны и статичны, нажимает на "Оплатить".

6

Пользователь подтверждает данные по платежу

7

Пользователь видит подтверждение платежа и выходит на главную страницу

8

Пользователь видит обновленный баланс цифрового тенге в Aitu Wallet

Анализ механизмов снижения риска двойных трат, отмывания денег и финансирования терроризма

Пилотная реализация базируется на принципах модели УТХО, где транзакция – это переход права владения токеном от одного пользователя к другому. На текущий момент для проведения офлайн транзакций используются токены из офлайн кошелька, которые в момент депозита получают подпись БВУ/ВУ, гарантирующую их подлинность.

При отсутствии интернета получатель платежа может проверить подлинность получаемых средств, проверив историю токена, передаваемую вместе с ним, вплоть до гарантирующей подписи банка. Когда один или оба участника транзакции выходят в онлайн, вся история токена из офлайн режима и все невалидированные платежные поручения передаются на ноды БВУ/ВУ участников и ноду нотариуса для финализации транзакций.

Валидация на уровне ноды нотариуса гарантирует проверку того, что токен ранее не был использован, митигируя риск двойной траты. Выявленный факт двойной траты в рамках офлайна должен передаваться в органы правопорядка для расследования и применения мер, определенных законодательством (равносильно подделке наличных денег).

При выборе технического решения для реализации «последней мили» в целевой платформе ЦТ в зависимости от выбранного решения необходимо проработать механизмы контроля двойных трат на уровне устройства.

Проверка транзакции на уровне БВУ/ВУ призвана гарантировать правомерность транзакций, так как даже в условиях настраиваемой пользователем анонимности БВУ/ВУ проводит KYC-проверки своих клиентов.

Для контроля риска отмывания денег и финансирования терроризма может использоваться программируемость токена на уровне его структуры и сверка права владения со специальными черными списками владельцев, поддерживаемыми НБРК на уровне платформы ЦТ. Практическое исследование AML/CFT не было фокусом R&D исследования офлайн платежей, но работа с риском была заложена в архитектуру платформы ЦТ и аналитически подтверждена возможность реализации.

Анализ возможных технологий для проведения цепочки транзакций в офлайне на основе удобства для пользователей

В рамках исследования проведен сравнительный анализ для определения **потенциала применения различных технологий передачи данных по мобильным устройствам** на основе удобства для пользователей.

Для исследования в R&D принято решение использовать комбинацию технологии QR и NFC, чтобы обеспечивать необходимый функционал и удобство для пользователя, а также сосредоточиться на основных целях текущего этапа, переиспользуя наработки PoC и MVP. В целевой картине рекомендуется продолжить исследование альтернативных технологий, чтобы повысить уровень UI/UX (бесконтактная передача с число действий клиента/за минимальный промежуток времени).

Анализ возможной длины цепочки офлайн транзакций

В рамках исследования проведен анализ факторов, влияющих на допустимую длину цепочки офлайн транзакций. С ростом числа офлайн транзакций, увеличивается объем передаваемой информации, что в конечном итоге влияет на время ее проведения.

Оценка допустимого объема токена офлайн транзакции с истории транзакций проводилась на основе:

- Структуры токена (необходимые данные для проведения офлайн транзакций)
- Закономерности возрастания истории офлайн токена (передача истории транзакций, как доказательство происхождения токена от точки депозита)
- Технологических ограничений (лимит технологии NFC в скорости передачи данных)
- Нефункциональных требований (время совершения транзакции)

По результатам практических экспериментов R&D и с учетом времени транзакции в 5 секунд допустимая длина истории токена составила 6-7 транзакций, что равнозначно 6-7 транзакциям, проведенным в офлайне с устройства одного пользователя, или 6-7 транзакциям, проведенным последовательно между разными устройствами пользователей. Потенциальная длина истории токена может быть выше за счет увеличения

скорости передачи данных, поддерживаемой выбранной технологией передачи данных на мобильных устройства, а также исследования механизмов сжатия передаваемых данных.

Технические требования и ограничения к устройствам поль-зователей для проведения офлайн транзакций

Для стабильной работы в офлайн режиме, принято решение использовать модели устройств с версиями ОС от Android 12 с поддержкой NFC/HCE (HCE - эмуляция хост карты). Для возможности работы в офлайн режиме (хранения истории транзакций и данных для проверок подписей) с учетом результатов по допустимой длине истории токена, необходимый дополнительный объём свободной памяти доступный на устройстве должен быть не менее 5,5-6 КБ, что является незначительным объемом данных по сравнению с размером самого приложения.

Анализ необходимости введения функциональных лимитов, приме-няемых к отдельному офлайн кошельку

По результатам исследования сделан вывод, что введение централизованных ограничений (ограничение на сумму для депозита, на максимальную сумму транзакции, на максимальное число транзакций и др.) технически реализуем, при этом сужает возможности пользователя, по сравнению с аналогом в виде наличных. Безопасность офлайн платежей также не возрастает при таких функциональных ограничениях. Рекомендуется на уровне банковского приложения в целевом решении предоставлять клиентам возможность выставить собственные лимиты по кошелькам (например, лимит на сумму трат за период).

Влияние офлайн транзакций на производительность нод

По итогам проведения офлайн транзакции на устройстве каждого из участников транзакции сохраняется платежное поручение, а также история транзакций, подтверждающая валидность текущей транзакции (текущего платежного поручения).

При выходе в онлайн, осуществляется синхронизация сгенерированных платежных поручений. Одно и тоже платежное поручение попадает в обработку на ноду несколько раз, поскольку отправляется разными участниками. При этом нода исполняет каждое платежное поручение только один раз. Чем больше участников в офлайне и чем больше транзакций они проведут, тем больше “дублей” платежных поручений попадет на ноды для обработки. Для обеспечения нефункциональных требований платформы, необходимо закладывать дополнительные требования к инфраструктуре с учётом нагрузки от офлайн транзакций, а также эффективные механизмы контроля дублей.

Подготовка к пилотированию

При подготовке системы к пилотированию были выявлены технологические особенности платформы Corda, влияющие на её производительность. При проведении тестов в качестве референтных значений по производительности использовались сопоставимые результаты по платежным системам со схожими характеристиками.

Использование ресурсов

Неоптимальное использование ресурсов может приводить к задержке обработки транзакций или даже к отказу системы. Были проведены тесты с замерами нагрузки оперативной памяти (RAM), процессора (CPU) на нодах банков и нотариуса. Результаты замеров показали, что ресурсы инфраструктуры используются оптимально.

Контейнеризация

Контейнеризация предназначена для оптимизации развертывания и CI/CD. Были проведены замеры проведения транзакций с и без контейнеризации нод по двум тестовым сценариям, тесты с использованием контейнеров показали улучшение показателей за счет оптимизации использования и управления ресурсами. Для работы в пилотном проекте было принято решение использовать контейнеризацию.

In memory (RAM) база данных

Альтернативные решения баз данных (БД) могут оптимизировать время резервного копирования при более быстрой обработке. Были проведены замеры PostgreSQL, БД, используемой в Corda Community edition по умолчанию, и in-memory БД на пилотной нагрузке.

Результаты замеров показали, что размещение БД в оперативной памяти дает незначительное улучшение по времени ответа и доле ошибок. При этом возникают такие риски, как ненадежность для производственной среды (когда база данных потребляет всю отведенную память, она прекращает обработку; в случае простоя сервера база данных стирается). В этом случае необходимо внедрять дополнительные механизмы резервного копирования, но они могут также повлиять на производительность. Также БД PostgreSQL по умолчанию не предназначена для использования в памяти (обычно используются Redis DB, Apache Ignite и другие, но они не являются базой данных Corda по умолчанию). Для работы в пилотном проекте продолжили использование БД по умолчанию.

Сравнение длительности обработки разных видов транзакций

Длительность обработки транзакции зависит от сложности заложенной в нее бизнес-логики. Пользовательские транзакции (переводы и покупки) являются одними из самых многосоставных в системе, их флоу состоят из большого количества обменов между нодами БВУ/ВУ, нотариальной нодой, а также криптографических вычислений (скрытие сумм, настраиваемая анонимность, подписи транзакций).

Сравнительные замеры длительности обработки пользовательских транзакций (покупок и переводов) и самой простой транзакции в системе (транзакции эмиссии) показали, что система выдерживает большую нагрузку и показывает лучшие показатели по времени ответа на простых транзакциях, чем на сложных. Максимальная нагрузка на простых транзакциях составила в несколько раз большее значение, чем на простых транзакциях, при сохранении целевого времени ответа.

Профайлинг транзакций

Были проведены замеры времени обработки каждого шага в процессе транзакции.

Результаты показали, что на нодах возникает **очередь из-за ограничения в один поток обработки данных в Corda Community Edition** и встроенных механизмов обработки флоу Corda. Также во время обработки каждой операции нода постоянно создает собственную резервную копию для аварийного восстановления. Несколько больших запросов к таблицам NODE_CHECKPOINTS (вставка, обновление, удаление) составляют более 75% всех обрабатываемых данных. В технической документации Corda этот процесс отмечен как процесс, создающий “узкое горлышко” для производительности [1]:

В этих таблицах наиболее интенсивная нагрузка чтения-записи, особенно в NODE_CHECKPOINTS и NODE_CHECKPOINT_BLOBS. В зависимости от используемых флоу и нагрузки на ноде, операции по этой таблице будут основным узким местом в производительности ноды.

Многопоточность

Несколько потоков для обработки запросов позволяет проводить больше операций в параллельном режиме в случае, если есть запас мощностей. В версии Corda Community есть заданное вендором ограничение на использование только 1 потока (single-thread only). В рамках Corda Enterprise реализована возможность настройки многопоточной обработки на нодах с помощью 2 параметров (rpcThreadPoolSize, flowThreadPoolSize); значения данных параметров вендор рекомендует устанавливать согласно инфраструктурным ресурсам (в зависимости от количества логических ядер). Были проведены замеры скорости обработки и доли ошибок на тестовых сценариях для нескольких конфигураций: Corda Community (1 поток) и Corda Enterprise (несколько потоков), пилотная нагрузка, нагрузка без допуска ошибок.

Результаты замеров показали, что многопоточность значительно улучшает показатели производительности в рамках проведенных тестов: позволяет в несколько раз увеличить пропускную способность и уменьшить среднюю задержку, снижает процент ошибок в запросах до незначительного уровня.

Выводы по итогам тестирования производительности при подготовке к пилотному проекту

Разработанная платформа ЦТ может работать как на базе Corda Community Edition (CCE), так и на базе Corda Enterprise Edition (CEE). На основе результатов и исследований нагрузочного тестирования выявлено, что на текущий момент **платформа покрывает требования по пропускной способности пилотного проекта**, но для достижения показателей в условиях промышленного масштаба необходимо реализовать ряд дополнительных задач по оптимизации производительности при разработке решения, как на базе CCE, так и на основе CEE.

Детализация возможного объема работ, а также рисков и затрат, связанных с выбором того или иного сценария развития платформы представлены в таблице ниже.

Версия Corda	Corda Community (CCE)	Corda Enterprise (CEE)
Потенциальный (неисчерпывающий) объем работ	<ul style="list-style-type: none"> Доработки в исходном коде для внедрения многопоточности и настраиваемого механизма обмена сообщениями между нодами Анализ ключевых факторов, влияющих на производительность, и тонкая настройка для достижения показателей промышленной платформы ЦТ 	Анализ ключевых факторов, влияющих на производительность, и тонкая настройка для достижения показателей промышленной платформы ЦТ
Преимущества	Полный контроль над разработкой, в том числе правами интеллектуальной собственности	<ul style="list-style-type: none"> Поддержка платформы вендором Переход на Corda 5 (после официального релиза версии) расширит возможности оптимизации производительности (модульный код, использование Kafka для сообщений, интеграция с Kubernetes)
Риски и затраты	<ul style="list-style-type: none"> Значительные трудозатраты по доработке исходного кода Создание ответвления от исходной версии – интеграция доработок версий Corda / миграция на более высокую версию становятся практически невозможными Полноценное функциональное и нагрузочное тестирование совместимости доработок с функциональностями ядра Corda платформы Отсутствие поддержки платформы вендором 	<ul style="list-style-type: none"> Стоимость лицензии Более высокая зависимость от вендора

Разработанная платформа ЦТ может работать как на базе Corda Community Edition (CCE), так и на базе Corda Enterprise Edition (CEE). На основе результатов и исследований нагрузочного тестирования выявлено, что на текущий момент платформа покрывает требования по пропускной способности пилотного проекта, но для достижения показателей в условиях промышленного масштаба необходимо реализовать ряд дополнительных задач по оптимизации производительности при разработке решения, как на базе CCE, так и на основе CEE.

На текущий момент наибольшее влияние на производительность решения оказывают:

- Наличие стандартных процессов Corda по резервному копированию, на которые приходится более 75% данных при обработке каждой транзакции;
- Наличие/отсутствие многопоточной обработки транзакций;
- Однопоточная обработка при проверке истории транзакций токена.

Дальнейшие рекомендации по оптимизации описаны в разделе технология внутреннего отчета:

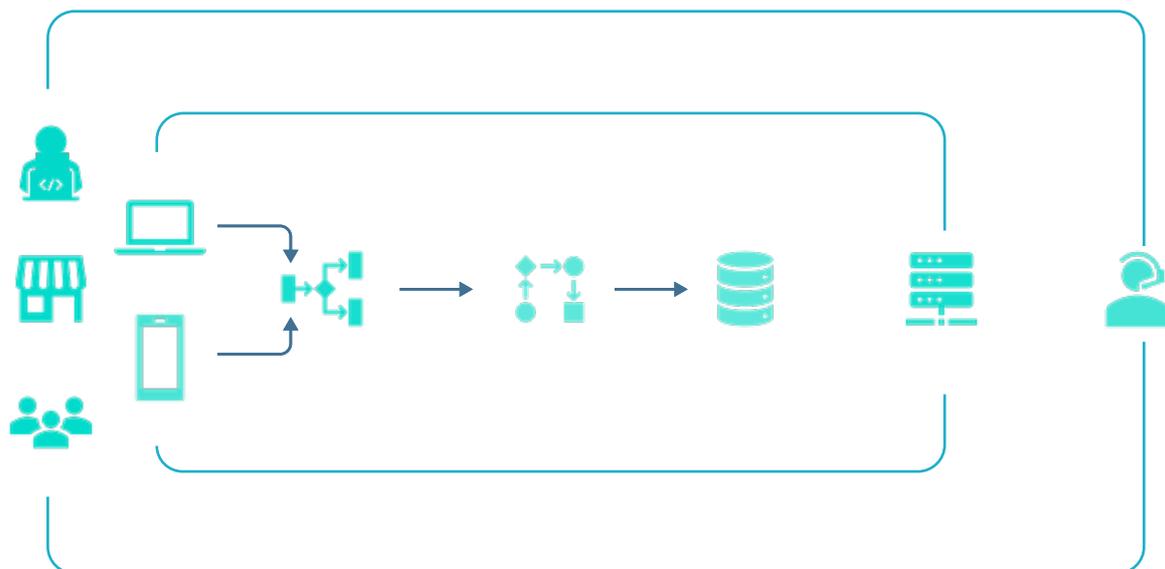
Целевая платформа ЦТ должна выдерживать высокие нагрузки за счет ее использования на уровне всего населения Казахстана, соответственно, важным подготовительным этапом для вывода решения в продуктив должно стать масштабное нагрузочное и стресс-тестирование и оптимизация производительности платформы для поддержания необходимых SLA.

Необходимо отметить, что заметного улучшения производительности можно достичь только за счет кумулятивного эффекта оптимизации на всех слоях решения.

В связи с тем, что фронтальные решения и мидл слой находятся в контуре внешних участников, важно настроить совместную работу и синхронизацию по результатам между всеми участниками платформы, а также выставить единые метрики производительности для отслеживания результата.

В качестве таких метрик могут выступать:

- количество транзакции, обрабатываемых в секунду ЦТ решением (платформа ЦТ + фронт-энд приложение);
- время обработки транзакции на стороне платформы ЦТ;
- время транзакции для пользователя (с учетом времени на обработки и отрисовку данных на фронт-энд приложении).



FRONT-END

Фокус на **пользовательском опыте** (клиентов, сотрудников) на основе общей производительности front-приложений и платформы

МИДЛ СЛОЙ

Индивидуальная оптимизация интеграции между front-end и back-end **специфичная для каждого приложения front-end**

BACK-END

Подход "**Test & try**" к настройке платформы для **баланса компромиссов** в функциональных и нефункциональных требованиях

БАЗА ДАННЫХ

Настройка оптимальной конфигурации БД **в сочетании с оптимизацией бэкенда**

ИНФРАСТРУКТУРА

Обеспечение **гибкости платформы** с учетом пиковых нагрузок, сезонных изменений и географии страны

ПОДДЕРЖКА

Базовые основы для обеспечения общей доступности, стабильности, работоспособности и надежности платформы

Производительность всего ЦТ решения (платформа ЦТ и фронтальные приложения) зависит от множества факторов как внешних по отношению к решению, так и заложенных в него бизнес-требований и технологических выборов. Требования к системе и технические факторы должны стать фокусом анализа и работы по отладке производительности.



В зависимости от результатов анализа преобладающих факторов могут применяться разные методы оптимизации производительности, а также различаться конкретные рекомендации внутри каждого метода.

	ФАКТОРЫ, ВЛИЯЮЩИЕ НА ПРОИЗВОДИТЕЛЬНОСТЬ	ВОЗМОЖНЫЕ МЕТОДЫ ОПТИМИЗАЦИИ (приоритет по простоте реализации и эффективности)
ТРЕБОВАНИЯ НБРК	Выбранные технологии для платформы (включая lastmile решения)	<ul style="list-style-type: none"> • Постоянный мониторинг зрелых/промышленных решений • Выбор решений на основе лучших практик и баланса между функциональными требованиями и результатами тестирования НФТ
	Протоколы криптозащиты	<ul style="list-style-type: none"> • Постоянная оптимизация пользовательского кода и настройка производительности в зависимости от меняющихся требований • Принятие решений по ключевым компромиссам (функциональная сложность VS производительность и стабильность VS безопасность)
	Алгоритм консенсуса	<ul style="list-style-type: none"> • Определение SLA в зависимости от критичности функциональности • Управление надежностью платформы
	Уровень конфиденциальности, количество скрытых данных	<ul style="list-style-type: none"> • Конфигурация балансировщика нагрузки • Оптимизация кода платформы DT (многопоточность, использование ресурсов, поиск данных) • Конфигурация хранения данных on- and off-ledger • Автоматическое вертикальное масштабирование • Оптимизация клиентского приложения (уменьшение числа запросов, пагинация, скелетная загрузка) • Event streaming • Кэширование (оба типа) • Горизонтальное масштабирование нотариусов и нод участников • Реализация BFF • Использование протокола HTTP2
	Сложность бизнес-логики платформы (например, смарт-контракты, программируемость, количество нод участвующих в транзакции, логика подтверждения транзакции, ...)	<ul style="list-style-type: none"> • Оптимизация кода платформы (сокращение цепочек транзакций)
РЕЗУЛЬТИРУЮЩИЕ ТЕХНИЧЕСКИЕ ФАКТОРЫ	Количество запросов	<ul style="list-style-type: none"> • Оптимизация БД (индексирование, конфигурация пула соединений, предварительно рассчитанные витрины данных, кластеризация)
	Глубина истории транзакций	<ul style="list-style-type: none"> • Оптимизация кода платформы (поиск данных)
	Сложность запросов к базе данных	<ul style="list-style-type: none"> • Управление надежностью платформы • Автоматическое вертикальное масштабирование • Горизонтальное масштабирование нотариусов и нод участников • Высокодоступные кластеры, поддерживаемые географически распределенными ЦОД
	Обработка офлайн транзакций	
	Стабильность платформы	

Принцип	Стратегические развилки	Технологические решения	Дизайн PoC	Дизайн MVP и R&D	Потенциальное видение
Подход к конфиденциальности	<p>Управление идентификацией:</p> <ul style="list-style-type: none"> • анонимность vs псевдоанонимность от НБРК и БВУ/ВУ • возможность использования анонимных кошельков 	<p>Интеграция с национальными универсальными сервисами:</p> <p>централизованное eKYC vs KYC проводится самостоятельно каждым БВУ/ВУ и интегрирован с eID</p>	<p>Первичная анонимность:</p> <p>Скрытие адресов на уровне ноды, что ограничивало функционал по подписанию транзакции клиентом с помощью одноразового stealth-адреса Сумма, записанная в токене, скрыта (гомоморфное криптографическое обязательство)</p>	<p>Дополнительный функционал:</p> <p>Анонимность на уровне транзакции с помощью stealth-адреса, функционал настраивается со стороны пользователя Сумма, записанная в токене, скрыта (гомоморфное криптографическое обязательство). Также формируется удостоверяющая Kernel подпись</p>	<p>Анонимность:</p> <p>Использование конфиденциальных вычислений (confidential computing) в доверенной среде исполнения кода (TEE) для сохранения конфиденциальности ключей пользователей</p>
Отслеживаемость истории транзакций	<p>• Отслеживаемость: полная анонимность (нет доступа к данным и истории транзакций) vs ограниченная, прослеживаемость со стороны НБРК или регулятора по запросу vs полная прослеживаемость со стороны НБРК, регулятора и БВУ/ВУ</p> <p>Управление счетами и кошельками: модель на основе токенов (token-based) vs модель на основе счетов (account-based) поверх модели на основе токенов (с дополнительными элементами управления учетной записью и возможностью программирования)</p>	<p>Безопасность: доступ к данным ограничен на уровне платформы ЦТ vs ограничен на уровне защищенных пространств (enclaves)</p>	<p>Прослеживаемость нодами:</p> <ul style="list-style-type: none"> • История транзакций токена от эмиссии • История транзакций хранится в хранилищах нод БВУ/ВУ 	<p>Дополнительный функционал:</p> <p>История транзакций “обрезается” при перевыпуске токена, с сохранением в хранилище ноды НБРК</p>	<p>Ограниченная прослеживаемость по запросу:</p> <p>Доступ к данным, необходимым для проведения мониторинга, расследований, ПОД/ФТ по запросу с помощью специального ключа</p>

Принцип	Стратегические развилки	Технологические решения	Дизайн PoC	Дизайн MVP и R&D	Потенциальное видение
Удобство использования ЦТ	<p>Свойства ЦТ: свойства наличных и токенизация права собственности (вкл. в случае потери связи - офлайн) vs электронные деньги</p> <p>Управление счетами и кошельками:</p> <ul style="list-style-type: none"> • Выбор модели кошельков • Использование всех токенов в офлайне vs отдельные офлайн кошельки <p>Ограничения использования в офлайне (временной интервал, число транзакций, сумма, ...)</p>	<p>Безопасность: уровень защиты от несанкционированного проникновения и взлома в офлайн режиме (алгоритмическая vs безопасность на основе аппаратного или программного обеспечения vs их комбинация)</p>	<p>Модель на основе токенов с хранением на устройстве пользователя</p> <ul style="list-style-type: none"> • Один пользователь = одно устройство • Максимум одна офлайн транзакция до синхронизации с нодой в онлайн 	<p>Модель на основе токенов с хранением на устройстве пользователя</p> <ul style="list-style-type: none"> • Один пользователь = одно устройство • Эксперименты с цепочками офлайн транзакций 	<p>Гибридная модель</p> <ul style="list-style-type: none"> • Отдельные кошельки – с поддержкой только онлайн-режима и с возможностью совершения офлайн транзакций • Отдельные офлайн кошельки для разных устройства пользователя <p>Использование защищенной среды исполнения кода (TEE) для хранения данных и исполнения кода</p>
Возможность восстановления ЦТ	<p>Управление кошельками:</p> <ul style="list-style-type: none"> • Выбор модели кошельков • Кто несет риск сбоя финансовых организаций (НБРК, используя отчетные данные для перевыпуска кошелька пользователя vs пользователи несут полную ответственность за свои кошельки в БВУ/ВУ) • Использование всех токенов в офлайне (сложное восстановление с юридической точки зрения) vs отдельные офлайн кошельки (онлайн-кошелек можно полностью восстановить) • Кто несет финансовые и юридические риски и обязательства по восстановлению кошелька (БВУ/ВУ (ограничения по онлайн или также по офлайн кошельку) vs пользователи (полное владение и ответственность)) 	<p>Безопасность и конфиденциальность:</p> <p>централизованная отчетность на уровне ноды НБРК vs отчетность в защищенном пространстве с доступом по запросу в НБРК</p>	<p>Модель без отчетных данных</p> <ul style="list-style-type: none"> • Единый онлайн и офлайн кошелек • Восстановление юридически сложно и должно быть дополнительно проработано • Пользователь рискует всеми ЦТ, предназначенными для использования в офлайне, в случае утери устройства 	<p>Модель без отчетных данных</p> <ul style="list-style-type: none"> • Отдельные кошельки – 1) с поддержкой только онлайн-режима, 2) с возможностью совершения офлайн транзакций • Пользователь рискует потерять ЦТ с офлайн кошелька, в случае утери устройства (процедура восстановления не предусмотрена) 	<p>Смешанная модель с отчетными данными</p> <ul style="list-style-type: none"> • Отдельные кошельки – 1) с поддержкой только онлайн-режима, 2) с возможностью совершения офлайн транзакций • Онлайн кошелек подлежит восстановлению, пользователь может запросить БВУ/ВУ заблокировать онлайн кошелек (в случае утери, фрода и др.) • Офлайн кошелек может быть восстановлен в случае проработки регуляторных аспектов <p>Регулярная отчетность и бэкапы пользовательских кошельков в хранилище ноды НБРК для устранения риска ошибки БВУ/ВУ или неправомерных действий</p>

Принцип	Стратегические развилки	Технологические решения	Дизайн PoC	Дизайн MVP и R&D	Потенциальное видение
Доступность для участников и работоспособность	<p>Роль участников рынка:</p> <ul style="list-style-type: none"> • Круг участников рынка и масштаб их участия • Централизованный контроль со стороны НБРК vs распределенная ответственность в рамках ограничений и шаблонов НБРК (НБРК определяет уровень доступа участникам) • Управление кошельками: модель на основе токенов vs модель на основе счетов поверх модели на основе токенов 	<p>Реализация программируемости: сеть полностью контролируется НБРК vs ограниченный доступ для некоторых участников (уровень доступа на уровне сети, уровень доступа на уровне релизов ...)</p>	-	<p>Первые эксперименты в песочнице R&D - участники имели возможность разрабатывать сценарии и тестировать гипотезы</p>	<ul style="list-style-type: none"> • Централизованные QA и CI/CD для смарт-контрактов предоставляются НБРК • Свойства счетов могут быть добавлены поверх модели на основе токенов для обеспечения доступа более широкому кругу участников

Принцип	Стратегические развилки	Технологические решения	Дизайн PoC	Дизайн MVP и R&D	Потенциальное видение
Безопасность ЦТ	<p>Партнерства:</p> <p>выбор подхода по офлайну и соответствующих партнеров (OS провайдеры, умные устройства, ...)</p>	<p>Безопасность:</p> <ul style="list-style-type: none"> • Алгоритмическая vs безопасность на основе аппаратного или программного обеспечения vs их комбинация • Подходы к обеспечению безопасности в онлайн и офлайне 	<p>Алгоритмическая безопасность</p> <p>Криптографические примитивы (на основе кривых Эдвардса)</p>	<p>Алгоритмическая безопасность</p> <p>Новый протокол проведения транзакций в офлайне (для реализации офлайн цепочек)</p>	<p>Комбинация подходов по безопасности</p> <ul style="list-style-type: none"> • Онлайн: конфиденциальные вычисления и использование криптографических библиотек, выпущенных государственными организациями РК • Офлайн: партнерство с поставщиками ОС и использование доверенной среды исполнения на устройствах для хранения данных и запуска криптографических примитивов
Производительность & доступность	<p>• Управление системой:</p> <p>централизованный перевыпуск токенов с длительной историей транзакций Нодой НБРК по запросу vs распределённый перевыпуск нодами БВУ/ВУ</p> <p>Платежная система:</p> <p>мгновенные платежи vs длительность транзакций в существующих платежных системах</p>	<p>Инфраструктура:</p> <ul style="list-style-type: none"> • Серверная vs облачная (kubernetes) <p>Ручное масштабирование серверов и сети vs использование автоматического масштабирования kubernetes</p>	-	<ul style="list-style-type: none"> • Перевыпуск токенов <p>Замеры пропускной способности на нагрузке Пилота</p>	<ul style="list-style-type: none"> • Использование event streaming внешних событий для балансировки нагрузки на API-запросы к сети DLT • Перевыпуск токенов с длинной историей транзакций и архивирование старых токенов (не находящихся в обращении) в хранилище ноды НБРК • Выбор технологии и механизма консенсуса, обеспечивающих горизонтальное масштабирование нод • Нагрузочное и стресс-тестирование системы на уровне продуктивной нагрузки (задержка, максимальная нагрузка)

Принцип	Стратегические развилки	Технологические решения	Дизайн PoC	Дизайн MVP и R&D	Потенциальное видение
Стабильность & наблюдаемость	<p>Управление системой: НБРК готов и способен гарантировать уровень стабильности платформы, юридически и финансово (quick-and-dirty vs продуманное и тщательно протестированное решение)</p>	<p>Инфраструктура: возможность создания географически распределенных центров обработки данных</p>	<p>Ограниченная функциональность ведения логов</p>	<p>Использование специализированных решений для логирования и мониторинга</p>	<ul style="list-style-type: none"> • Создание кластеров высокой доступности (географически распределенные центры обработки данных) • Тестирование SLA доступности для продуктивного этапа • Проверка плана восстановления данных, резервного копирования и процедур миграции • Круглосуточная поддержка и управление инцидентами (на основе инструментов оповещения, мониторинга, логирования)

Приложение 2

Выбор метода опроса (веб-опрос)

Для построения микромоделей оценки эластичности замещения цифрового тенге и определения потенциального спроса на разрабатываемую национальную цифровую валюту, NAC Analytica был проведен веб-опрос казахстанцев на заданную тему (с квотированием по регионам).

Метод проведения опроса был выбран не случайно, а основывался на мировой практике в данной сфере. Практически во всех исследованиях, касающихся вопросов изучения платежных инструментов и цифровой валюты, доминирующим методом опроса являлся количественный метод в режиме онлайн/веб-опрос. Например, опросы населения в Канаде (Carlos Arango and Angelika Welte 2012), (Christopher S. Henry and Kim P. Huynh and Angelika Welte 2018), (Marie-Hélène Felt and David Laferrière 2020), Великобритании (Natalie Ceeney 2018), Нидерландах (Vijlsma et al. 2021), России (Centre for Research in Financial Technologies and Digital Economy SKOLKOVO-NES 2019) проводились именно в режиме онлайн/веб опроса с использованием квотирования. Кроме того, международные сравнительные исследования в развитых и развивающихся странах (OMFIF 2020), (OMFIF 2021) также проводились данным методом.

Выбор метода опроса этими странами и организациями был определен спецификой исследовательского вопроса. Так, результаты многочисленных репрезентативных исследований в разных странах показали, что самой активной группой пользователей банковских услуг являются лица в среднем до 45 лет, проживающие в городской местности и имеющие высшее образование. Таким образом, параметры целевой аудитории потенциальных пользователей цифровой валюты совпадали с параметрами активных пользователей Интернет-пространства, в связи с чем и был выбран метод онлайн сбора данных.

Следует отметить, что опыт других стран показал, что режим проведения опроса в данной сфере не оказывает существенного влияния на результаты. Так, канадские исследователи проводили опросы как в режиме онлайн, так и путем репрезентативного телефонного опроса, и

результаты показали объективность и надежность данных, полученных в этих двух режимах (при сравнении опросов между собой).

Что касается Казахстана, то в нашей стране также применим данный метод, так как по официальным данным, доля пользователей Интернета уже превышает 90%.

В целом нужно отметить, что режим веб-опроса имеет ряд преимуществ, таких как быстрота сбора данных, более низкая стоимость проведения по сравнению с другими методами, отсутствие влияния интервьюера на результаты опроса, а также обеспечение максимальной анонимности респондентов.

Микроэконометрический анализ на основе модели структурного спроса Li (2021). позволил оценить потенциальный спрос на ЦТ в Казахстане по сравнению с его близкими альтернативами. ЦТ, наличные деньги и депозиты считаются группой продуктов с различными атрибутами/характеристиками. Выгоды домохозяйств от владения каждым продуктом зависят от таких характеристик продукта, как удобство, стоимость использования, безопасность, уровень повсеместного принятия, анонимность, бюджетирование, характеристики домохозяйств и ненаблюдаемые индивидуальные предпочтения домохозяйств. Проведена оценка предпочтений домохозяйств по каждому продукту на основе опросных данных. Ответы содержат информацию о долях наличных денег и депозитов в ликвидных активах. Также респонденты ставили свои рейтинги по характеристикам продуктов. Далее предполагая, что предпочтения людей остаются неизменными после выпуска ЦТ, спрос на ЦТ прогнозировался на основе его характеристик дизайна и оценки каждого атрибута домохозяйствами.

В рамках той же модели оценивалась постоянная эластичность замещения между ЦТ и денежными средствами. Методология оценки эластичности замещения основывается на том, что домохозяйства получают полезность от хранения наличных денег, депозитов и ЦТ. Допуская, что наличные деньги и ЦТ являются близкими заменителями, функция полезности с постоянной эластичностью замещения домашних хозяйств состоит из хранения наличных денег, депозитов и ЦТ.

При условии бюджетного ограничения ликвидных активов домохозяйства состоящий из суммы всех наличных денег, депозитов и ЦТ. Уравнение эластичности замещения между наличными и ЦТ выведено решением условий первого порядка уравнения Лагранжа, согласно Li (2021). Так как ЦВЦБ является новым понятием для всего мира в последние несколько лет, экономические исследования на данную тему ограничены. Международный обзор литературы показал, что эмпирической оценки эластичности замещения между ЦВЦБ и наличными еще не проведено, но теоретические исследования в рамках DSGE моделей существуют.

Вероятность принятия ЦТ прогнозировалась с помощью логистической регрессии. Успех внедрения ЦТ зависит от понимания того, какие качества платежных инструментов являются наиболее важными с точки зрения потребителей, а также факторов, повышающих вероятность использования ЦТ.

Чтобы изучить отношение потребителей к внедрению ЦТ, построена модель логистической регрессии, которая оценивает влияние различных социально-демографических факторов, знание ЦТ, осведомленность о криптовалютах, важность различных характеристик ЦТ, удобство использования наличных и анонимность, доверие к собственному банку и Национальному банку Казахстана. Кроме того, анализируются потребители, которые часто используют наличные и мобильные приложения для совершения платежей. Зависимой переменной является готовность респондента использовать ЦТ. Переменная построена на основе вопроса опроса: «Если завтра в Казахстане будет введен цифровой тенге, с какой вероятностью вы бы им воспользовались?». Это двоичная переменная, которая принимает значения 1 для ответов респондентов «Определенно да» или «Скорее да» и 0 для вариантов ответов «Не уверен» или «Скорее нет» или «Определенно нет».

	Удобство	Стоимость	Безопасность	Анонимность	Принятие	Бюджетирование	Банковская комплектация	Процент по депозиту
Базовый дизайн	Наличные	Наличные	Наличные	0,7	1	0,7	0	0
Дизайн как у наличных	Наличные	Наличные	Наличные	1	1	1	0	0
Дизайн как у карты	Банковская карта	Банковская карта	Банковская карта	0	Банковская карта	0	1	Депозитная ставка

Примечание:

1. Где указаны значения, Вес означает вес на переменные в общей функции потерь.
2. Значения в таблице распределены от 1 до 4, где «1» наиболее стабильный сценарий, а «4» – наименее стабильный

Объем производства и уровень инфляции											
Сценарий/Вес	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	1	1	1	1	1	1	1	1	1	1	1
Выпуск ЦТ как 10% от ВВП	2	2	2	3	4	4	4	4	4	4	4
ЦТ с фиксированной ставкой в 2%	3	3	3	2	2	2	2	2	2	2	2
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	4	4	4	4	3	3	3	3	3	3	3

Объем производства и реальный обменный курс											
Сценарий/Вес	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	1	1	1	1	1	1	1	1	1	1	1
Выпуск ЦТ как 10% от ВВП	4	4	4	4	4	4	4	4	4	4	4
ЦТ с фиксированной ставкой в 2%	2	2	2	2	2	2	2	2	2	2	2
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	3	3	3	3	3	3	3	3	3	3	3

Объем производства и дефицит бюджета

<i>Сценарий/Вес</i>	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	1	1	1	1	1	1	1	1	1	1	1
Выпуск ЦТ как 10% от ВВП	2	2	2	2	2	2	2	2	2	2	4
ЦТ с фиксированной ставкой в 2%	4	4	4	4	4	4	4	4	4	3	2
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	3	3	3	3	3	3	3	3	3	4	3

Примечание:

1. Где указаны значения Вес означает вес на переменные в общей функции потери
2. Значения в таблице распределены от 1 до 4, где «1» наиболее стабильный сценарий, а «4» означает наименее стабильный

Достаточность капитала											
<i>Сценарий/Вес</i>	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	2	2	2	2	2	2	2	2	2	2	2
Выпуск ЦТ как 10% от ВВП	1	1	1	1	1	1	1	1	1	1	1
ЦТ с фиксированной ставкой в 2%	3	3	3	3	3	3	3	3	3	3	3
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	4	4	4	4	4	4	4	4	4	4	4

Рентабельность активов											
<i>Сценарий/Вес</i>	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	2	2	2	2	2	2	2	2	2	2	2
Выпуск ЦТ как 10% от ВВП	1	1	1	1	1	1	1	1	1	1	1
ЦТ с фиксированной ставкой в 2%	3	3	3	3	3	3	3	3	3	3	3
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	4	4	4	4	4	4	4	4	4	4	4

Рентабельность капитала

<i>Сценарий/Вес</i>	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
ЦТ с нулевой процентной ставкой	2	2	2	2	2	2	2	2	2	2	2
Выпуск ЦТ как 10% от ВВП	1	1	1	1	1	1	1	1	1	1	1
ЦТ с фиксированной ставкой в 2%	3	3	3	3	3	3	3	3	3	3	3
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	4	4	4	4	4	4	4	4	4	4	4

Примечание:

1. Значения в таблице распределены от 1 до 2, где «1» означает, что отклики важных макроэкономических и финансовых переменных менее выражены от базового сценария без ЦТ.
2. Значение «2» означает, что отклики более выражены от базового сценария. Так же значение «2» дается сразу нескольким сценариям, так как отклики в данных сценариях сопоставимы между собой.

Сценарий/Шок	Макроэкономическая стабильность		Финансовая стабильность	
	ДКП	Цена на нефть	ДКП	Банковский капитал
ЦТ с нулевой процентной ставкой	1	1	2	2
Выпуск ЦТ как 10% от ВВП	2	2	1	1
ЦТ с фиксированной ставкой в 2%	2	2	2	2
ЦТ с варьируемой ставкой, где процентная ставка определяется через правило Тейлора	2	2	2	2

DSGE модели для оценки влияния на макроэкономику, финансовую стабильность

Используя оценку постоянной эластичности замещения, ЦТ внедрен в среднемасштабную модель динамического стохастического общего равновесия (DSGE) для Казахстана для анализа механизмов передачи шоков и последствия ЦТ для макроэкономической стабильности и благосостояния домохозяйств, измеряемые функцией потерь.

Была построена модель DSGE с банковским сектором для анализа механизмов передачи финансовых шоков при наличии ЦТ и анализа влияния внедрения ЦТ на финансовую стабильность.

Для анализа влияния потенциального внедрения ЦТ на макроэкономические и финансовые переменные необходимо построить теоретическую модель экономики Казахстана, так как эмпирические модели требуют наблюдений на экономику с ЦТ на достаточно длинный период времени. Из-за новшества ЦТ в экономике и отсутствия наблюдений на экономику с цифровой валютой были строим DSGE модели для Казахстана, в которых домохозяйства используют ЦТ как платежное средство наряду с наличными и безналичными денежными средствами. Эти модели позволяют нам экспериментировать альтернативные варианты внедрения ЦТ внутри моделей и измерять их влияние на макроэкономические и финансовые переменные в равновесии. Микроэконометрически модели, в свою очередь, позволяют нам оценить постоянную эластичность замещения между ЦТ и денежными средствами в Казахстане, и использовать этот параметр внутри DSGE моделей.

То есть, новшество данного исследования заключается в том, что модели учитывают не только уникальную структуру экономики Казахстана через уравнения, но также учитывают специфическое восприятие домохозяйствами ЦТ и денежных средств в Казахстане. По сравнению с другими исследованиями по ЦВЦБ в DSGE-моделях, мы оцениваем постоянную эластичность замещения через микроэконометрическую модель и используем в DSGE-модели, в то время как остальные исследования фиксируют коэффициент эластичности замещения на значениях, не подкрепленными эмпирическими оценками.

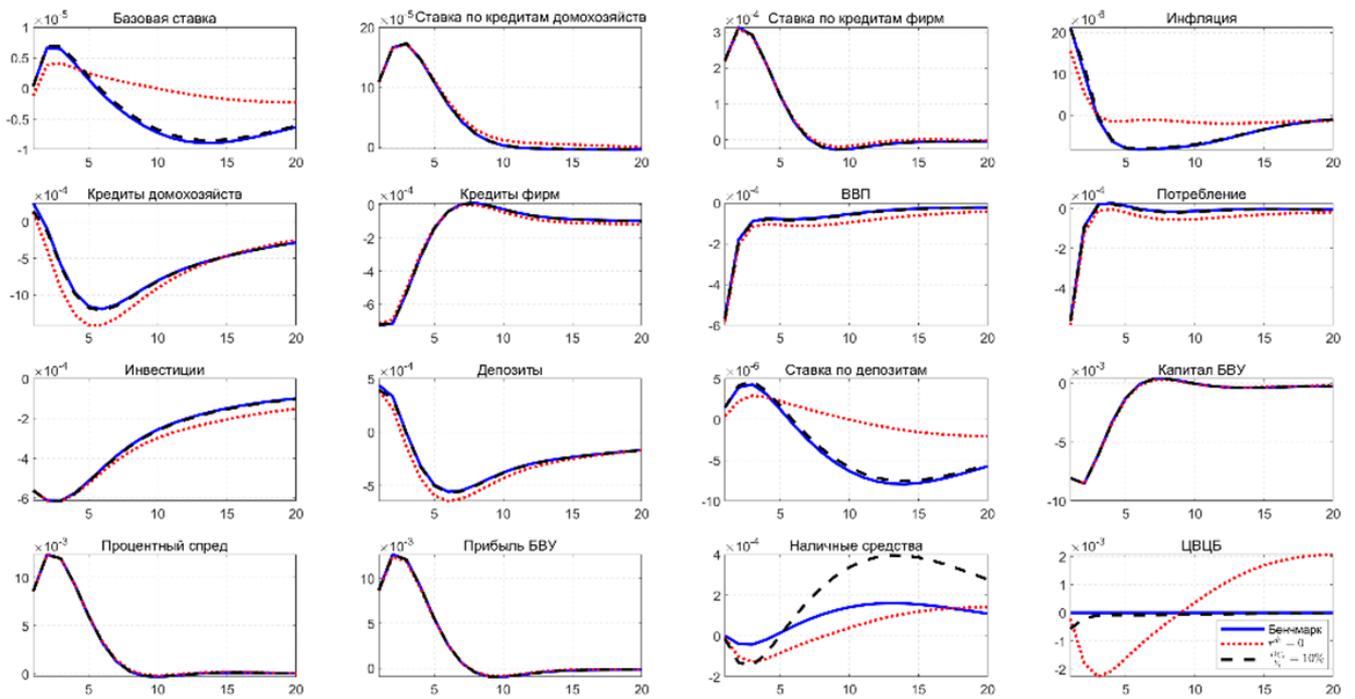
В целом существует лишь ограниченное количество работ, анализирующих наличие ЦВЦБ в модели DSGE. Barrdear and Kumhof (2021) анализируют макроэкономические последствия и влияние на благосостояние внедрения ЦВЦБ с использованием модели закрытой экономики DSGE, откалиброванной для экономики США. Они приходят к выводу, что ВВП растет на 3% в устойчивом состоянии при внедрении ЦВЦБ. Однако модель закрытой экономики менее актуально для Казахстана, поскольку наша экономика более подвержена внешним шокам, что делает актуальным рассмотрение в модели особенностей открытой экономики. George et al. (2018) и Minesso et al. (2022) строят DSGE-модели открытой экономики с ЦТ для анализа механизмов передачи шоков в зависимости от характеристик ЦВЦБ. Minesso et al. (2022) приходят к выводу, что внедрение ЦВЦБ в Еврозоне приведет к более волатильному обменному курсу евро по отношению к остальным валютам. Burlon et al. (2022) строят DSGE-модель с финансовым сектором и ЦВЦБ. Они приходят к выводу, что ВВП падает в реальном выражении в устойчивом состоянии для Еврозоны при внедрении ЦВЦБ, но также наблюдают сглаживание отклика кредитования и ВВП на шоки в экономике. Gross and Schiller (2021) также изучают влияние ЦВЦБ на банковский сектор в экономике. Они приходят к заключению, что ЦВЦБ может вытеснить депозиты банков, но центральный банк сможет контролировать данный отток средств из депозитов в ЦВЦБ меняя процентную ставку на ЦВЦБ. В настоящем отчете мы основываемся на существующих моделях DSGE - Abilov and Rahardja (2022) и Gerali et al. (2010) и модифицируем их, включая ЦВЦБ в модели. Данные модели используются в этом отчете для анализа экономических последствий внедрения ЦТ в Казахстане.

Механизмы передачи финансовых шоков практически неизменны из-за близкой взаимозаменяемости наличных средств и ЦТ. Импульсные отклики ключевых макроэкономических переменных в базовом сценарии без ЦТ и в сценариях с ЦТ отличаются только величиной, но не направлением импульсных откликов. С точки зрения финансовой стабильности оптимальный размер ЦТ составляет 10% от годового ВВП. С другой стороны, правило ЦТ с нулевой процентной ставкой по ЦТ приводит к улучшению макроэкономической среды по сравнению с другими правилами ЦТ, поскольку

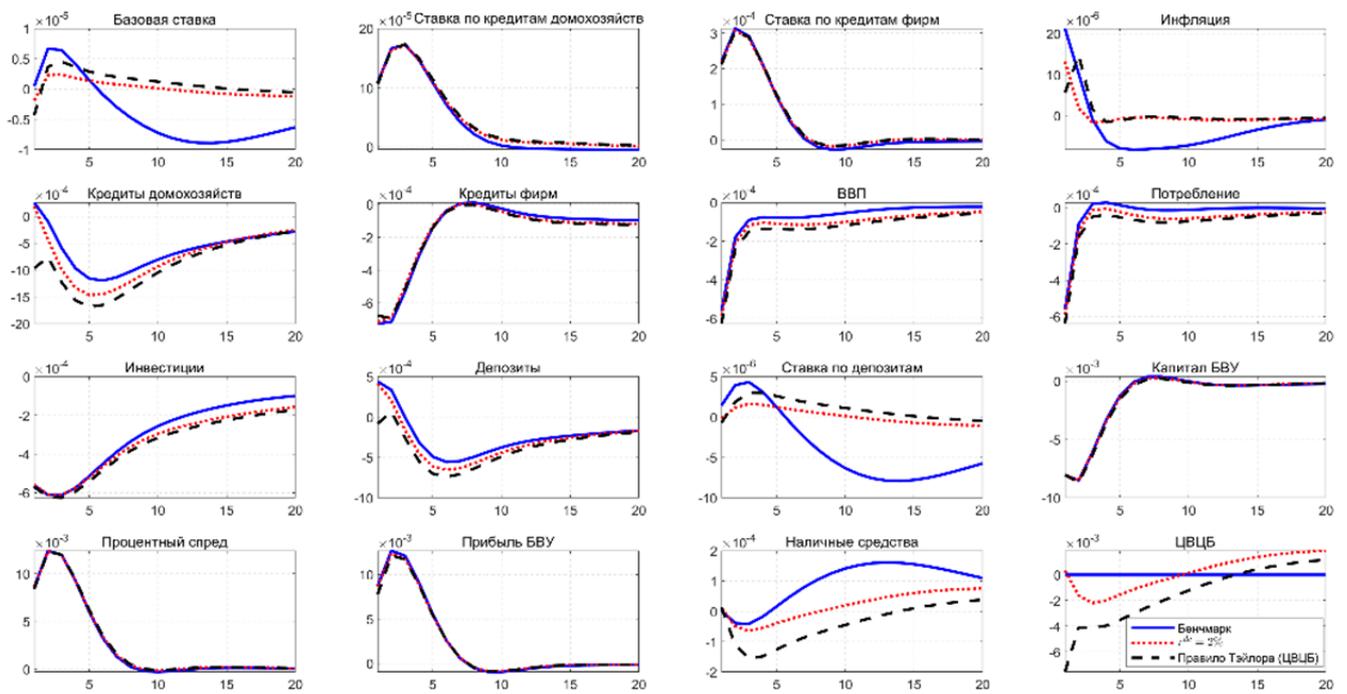
экономика более стабильна, а благосостояние домохозяйств меняется незначительно.

Рисунок показывает, что внедрение ЦТ позволяет центральному банку влиять на экономику посредством выпуска и изъятия ЦТ из экономики. В этом случае из-за несовершенной взаимодополняемости (постоянная эластичность меньше 1 и равна 0,735) наличные средства и ЦТ движутся синхронно, в связи с чем ликвидность в экономике реагирует сильнее. Т.е. когда меняется базовая ставка, также меняются издержки хранения активов в наличных средствах и ЦТ. Поэтому изменение базовой ставки приводит к изменению объема денежных средств и ЦТ, необходимых домохозяйствам. Но так как они взаимодополняемые виды инструментов, изменение в одном подстегивает изменение в другом инструменте в одинаковом направлении, т.е. создается эффект обратной связи (feedback effect). Другими словами, когда центральный банк меняет базовую ставку, объем ликвидности меняется сильнее из-за взаимодополняемости денежных средств и ЦТ. В результате банки реагируют, меняя ставки по кредитам в большей степени, что приводит к более выраженным изменениям в потреблении и инвестициях. В свою очередь, это приводит к более выраженной реакции ВВП и инфляции в экономике. По сути, усиление реакции макроэкономических переменных на базовую ставку означает, что при внедрении ЦТ центральный банк может оказывать большее влияние на экономику.

На рисунках показаны импульсные отклики выбранных переменных на отрицательный шок банковского капитала в соответствии с базовым сценарием и четырьмя альтернативными сценариями с ЦВЦБ. Отклики при нулевой процентной ставке по ЦВЦБ и фиксированном соотношении ЦВЦБ к ВВП почти идентичны импульсным откликам по базовому сценарию. Разница возникает в откликах наличных средств и ЦВЦБ. С другой стороны, сценарии с фиксированной процентной ставкой по ЦВЦБ и правилом Тейлора для процентной ставки по ЦВЦБ демонстрируют незначительную разницу в величинах импульсных откликов эндогенных переменных. Тем не менее направления импульсных откликов аналогичны базовому сценарию. Отрицательный шок банковского капитала ухудшает соотношение капитала к активам банков. Следовательно, они реагируют повышением ставок по депозитам и кредитам. Более высокие процентные ставки по депозитам привлекают сбережения вкладчиков и компенсируют банкам потерю собственного капитала. Более высокие процентные ставки по кредитам увеличивают спред и приводят к увеличению прибыли банков, которая может быть использована для накопления банковского капитала. С другой стороны, более высокие процентные ставки снижают спрос на кредиты со стороны заемщиков и предпринимателей. В результате мы наблюдаем снижение частных инвестиций и потребления. Однако негативное влияние на потребление быстро исчезает в течение 3 кварталов из-за низкой жесткости. Тем не менее объем производства и инвестиции остаются ниже своих устойчивых значений в течение более длительного периода. Инвестиции возвращаются в устойчивое состояние только через 20 кварталов. Инфляция повышается в ответ на увеличение предельных издержек фирм из-за снижения накопления капитала и более высокого спроса на услуги рабочей силы. Центральный банк реагирует повышением базовой ставки, чтобы противостоять эффекту растущей инфляции. Во всех сценариях с ЦВЦБ, за исключением сценария с фиксированным соотношением ЦВЦБ к ВВП, наличные средства и ЦВЦБ подвержены корректировке после исчезновения эффекта шока, в то время как при ЦВЦБ на уровне 10% от ВВП данные ликвидные активы корректируются гораздо быстрее в течение 5 кварталов.



Импульсные отклики при повышении базовой ставки



Импульсные отклики на отрицательный шок капитала ББУ

Подходы стран для устранения рисков

Согласно последним исследованиям BIS, предлагаемые меры для устранения рисков перетока средств в ЦВЦБ группируются на две категории: количественные и ценовые меры.

Варианты проектирования ЦВЦБ			
Количественные меры/ограничения	Максимальный лимит хранения	Дифференцированные лимиты	Лимиты на транзакции
Ценовые показатели/вознаграждения	Без вознаграждения/ Отрицательное вознаграждение		Многоуровневое вознаграждение
Антикризисные меры	Коридор/лимиты на конвертацию		Банковская поддержка

Количественные меры ограничат использование ЦВЦБ путем введения ограничений на передачу и/или хранение ЦВЦБ. Количественные ограничения могут быть либо на основе общего объема (центральные банки ограничивают количество ЦВЦБ, хранящихся у физических лиц/владельцев индивидуальных счетов), либо на основе потоков (ограничения на количество ЦВЦБ, которые могут быть переведены в течение определенного периода времени, например, в день, владельцем счета). Уровни количественных лимитов могут быть установлены с учетом объема оборота наличных денег и платежей в домашних хозяйствах.

Ценовые меры могут быть использованы для снижения объема хранения ЦВЦБ или крупных платежей в ЦВЦБ (без их ограничения). Система вознаграждения может быть как одноуровневой, так и многоуровневой. В одноуровневой системе владельцы ЦВЦБ будут вознаграждаться по ставке независимо от удерживаемой суммы. В двухуровневой системе, до заранее определенной пороговой суммы (q_1), ЦВЦБ владельцы будут выплачивать определенную прибыль (r); сумма, удерживаемая сверх q_1 , будет вознаграждена с более низкой доходностью ($r_2 < r_1$). Центральным банкам необходимо будет принимать решения о том, как применять процентные ставки (например, на спотовой основе или в среднем за период), принимая во внимание технические возможности. Кроме того, центральные банки могли бы рассмотреть возможность взимания комиссии (фиксированной или прогрессивной) за переводы ЦВЦБ, превышающие определенную сумму.

Также рассматриваются комбинации мер. Например, центральный банк мог бы рассмотреть

двухуровневую систему вознаграждения с ограничениями на сумму ЦВЦБ, которая может быть переведена в определенный день. Независимо от того, будет ли внедрена параллельно или нет, наличие вышеуказанных конструктивных особенностей снизит привлекательность ЦВЦБ как инструмента сбережения и таким образом, уменьшит степень дезинтермедиации и возможные последующие риски финансовой стабильности.

Ограничения также могут применяться по-разному для разных владельцев счетов ЦВЦБ, для предпринимателей и домашних хозяйств. Например, более жесткие ограничения для бизнеса могут снизить общий объем использования ЦВЦБ, сохраняя при этом доступ к финансовым услугам для обычных граждан.

Такие ограничения могут вводиться на постоянной основе или на временной основе. Некоторые центральные банки могут рассмотреть возможность структурного ограничения масштабов использования ЦВЦБ и рисков, связанных с заменой частными деньгами. Другие могут предпочесть использовать меры только на переходном этапе, чтобы замедлить первоначальное освоение и дать время финансовой системе адаптироваться.

Центральные банки будут оценивать необходимый объем ЦВЦБ с учетом рисков перетока средств из текущих счетов и депозитов в ЦВЦБ - этот уровень может варьироваться в зависимости от юрисдикции и ее финансовой структуры. Все ограничения будут учитывать основополагающие цели внедрения ЦВЦБ, предоставление населению доступа к безопасным средствам оплаты,

расширение охвата и доступности или стимулирование конкуренции вокруг ЦВЦБ, которые являются частью его экономической выгоды.

Внедрение лимитов требует доступа к соответствующим данным (даже если они автоматизированы) и дополнительной обработки. В некоторых случаях могут возникать правовые и политические вопросы, требующие рассмотрения в связи с предпосылкой введения ограничений и/или отрицательных процентных ставок на имущество домашних хозяйств, принадлежащее населению.

Меры по управлению банковским риском

Пруденциальное регулирование постоянно пересматривается, поскольку ликвидность банковских депозитов и других обязательств меняется с течением времени, например, из-за технологических инноваций. Внедрение ЦВЦБ или новых форм частных денег, таких как стейблкоины, может повлиять на скрытый риск системных запусков, и банкам также может потребоваться адаптировать свою собственную практику (Juks (2018)). Например, в действующих правилах LCR параметры оттока депозитов, предоставляемых розничными клиентами и клиентами малого бизнеса, были установлены на основе наблюдаемых темпов оттока в периоды стресса, которые по определению не учитывают влияние на поведение вкладчиков в условиях стресса в присутствии ЦВЦБ или некоторых новых частных форм цифровых денег. Если введение ЦВЦБ увеличит риск оттока для таких депозитов, возможно, потребуется пересмотреть соответствующие ставки оттока, чтобы обеспечить достаточную ликвидность для покрытия потенциальных оттоков во время стресса.

Властям также могут потребоваться более оперативные инструменты управления кризисными ситуациями и пересмотр антикризисных мер, таких как ограничения или контроль за оттоком средств с банковских депозитов. Рамки предоставления ликвидности центральные банки также могут быть пересмотрены, например, для расширения обеспечения или доступа.

Другие меры

В той мере, в какой внедрение ЦВЦБ или новых частных форм цифровых денег вводит новые тенденции, стратегии, положения, правила или новые конкурентные преимущества в предоставлении услуг различными игроками, могут возникнуть новые концентрации предоставления услуг. Центральные банки должны быть уверены в том, что нормативно-правовая база и механизмы надзора будут способствовать эффективному мониторингу и регулированию по мере развития системы.