



НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

# ПРОЕКТ ЦИФРОВОЙ ТЕНГЕ



ДОКЛАД О РЕЗУЛЬТАТАХ ПИЛОТНОГО ПРОЕКТА

2021

# Сокращения

<b>AML/CFT (ПОД/ФТ)</b>	(Anti-money laundering, Combating the financing of terrorism) Противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма
<b>API</b>	(Application programming interface) Программный интерфейс приложения – описание способов, которыми одна компьютерная программа может взаимодействовать с другой программой
<b>DeFi</b>	(Decentralised Finance) Децентрализованные финансы – отрасль финансовых услуг на основе технологий распределенного реестра и смарт-контрактов
<b>DLT</b>	(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
<b>IoT</b>	(Internet of things) Интернет вещей – совокупность технологий, объединяющих устройства в сеть и позволяющих им собирать, анализировать, обрабатывать и передавать данные другим объектам через программное обеспечение, приложения или технические устройства, например, инициировать банковские транзакции
<b>KYC</b>	(Know your customer или Know Your Client) Знай своего клиента – процедура идентификации личности клиента
<b>P2P</b>	(Peer-to-Peer, Person-to-Person) Платежи и переводы денежных средств между физическими лицами
<b>UTXO</b>	(Unspent transaction output) Вывод неизрасходованных транзакций, т.е. остатки криптовалюты, которые пользователь получает с каждой транзакции. Используется в системе блокчейна.
<b>БВУ</b>	Банк второго уровня
<b>ГУ</b>	Государственное учреждение
<b>МСПД</b>	Межбанковская система переводов денег - платежная система, предназначенная для осуществления платежей и (или) переводов денег между ее участниками с использованием денег, находящихся на корреспондентских счетах, открытых в НБРК, путем индивидуального исполнения каждого указания ее участника с завершением переводов денег в течение операционного дня
<b>НБРК</b>	Национальный Банк Республики Казахстан
<b>СМК</b>	Система межбанковского клиринга - платежная система, предназначенная для осуществления платежей и (или) переводов денег между ее участниками-банками, организациями, осуществляющими отдельные виды банковских операций, путем многостороннего клиринга указаний участников
<b>СМП</b>	Система мгновенных платежей - платежная система, предназначенная для круглосуточного осуществления платежей и (или) переводов денег между ее участниками, с использованием денег, находящихся в НБРК, с обеспечением мгновенного зачисления денег в пользу бенефициара платежа и (или) перевода денег
<b>ТСП</b>	Торгово-сервисное предприятие
<b>ЦБ</b>	Центральный банк
<b>ЦВЦБ</b>	Цифровая валюта центрального банка
<b>ЦТ</b>	Цифровой тенге

# Глоссарий

<b>Доклад</b>	Доклад для публичных обсуждений «Цифровой тенге» (май 2021)
<b>Интероперабельность</b>	Способность продукта или системы, интерфейсы которых полностью открыты, взаимодействовать и функционировать с другими продуктами или системами без ограничений доступа и реализации
<b>Консенсус</b>	Набор определенных математических правил и функций, регулирующих работу сети. Консенсус обеспечивает целостность и безопасность транзакций в распределенном реестре благодаря подписанию и валидации транзакций всеми участниками этих транзакций.
<b>Легкие клиенты платформы</b>	Участники (ноды) сети, которые могут участвовать в транзакциях и самостоятельно полноценно подписывать их, при этом это участники с ограниченной функциональностью относительно полноценных клиентов платформы (в части хранения полной копии реестра, валидации транзакций и возможности добавления и запуска приложений Corda)
<b>Нода</b>	Узел сети – устройство, соединенное с другими устройствами как часть сети
<b>Опрос</b>	Опрос будущих потенциальных пользователей ЦТ и платформы ЦТ для определения свойств цифрового тенге. Был проведен в ходе пилотного проекта для выявления необходимых характеристик ЦТ и токенов ЦТ в частности.
<b>Оффлайн-платежи / покупка в режиме оффлайн / оффлайн-покупка / оффлайн-транзакция</b>	В данном документе: платежи при отсутствии интернет соединения у обоих участников транзакции
<b>Пилотная платформа</b>	Прототип платформы цифрового тенге с ограниченным количеством эмулируемых участников, предназначенный для тестирования основных сценариев жизненного цикла ЦТ
<b>Пилотный проект</b>	Проект по разработке прототипа платформы (пилотной платформы) для проверки жизнеспособности концепции цифрового тенге
<b>Программа</b>	Программа развития национальной платежной системы в Республике Казахстан до 2025 года
<b>Распределенный реестр</b>	Набор баз данных с финансовыми транзакциями и механизмами учета этих транзакций, основанными на криптографических функциях
<b>Смарт-контракт</b>	Компьютерный алгоритм, запрограммированный договор, условия которого прописаны в программном коде и который автоматически исполняется с помощью технологии блокчейна
<b>Токен</b>	Состояние записи в реестре на определенный момент времени, ценность токена заложена в нем самом и подтверждается криптографическими операциями в рамках распределенного реестра
<b>Экосистема</b>	В данном документе: совокупность процессов взаимодействия с внешними участниками рынка в рамках пилотного проекта

# Содержание

<b>Благодарность, отзывы</b>	<b>5</b>
<b>Резюме</b>	<b>6</b>
<b>Введение</b>	<b>7</b>
<b>1. Предпосылки и развитие ЦВЦБ в Казахстане</b>	<b>10-23</b>
1.1 Исторические предпосылки и тренды в платежной индустрии	10
1.2 ЦВЦБ в сравнении с другими формами денег	12
1.3 Преимущества и возможности ЦВЦБ	14
1.4 ЦТ: предпосылки и подход к внедрению	15
<b>2. Результаты пилотного проекта</b>	<b>25-69</b>
2.1 Обзор пилотного проекта ЦТ	25
2.2 Роли, участники и архитектура пилотной платформы	29
2.3 Выбор технологического решения (DLT-платформы)	32
2.4 Сценарии пилотного проекта	33
2.5 Технологические аспекты для дальнейшей проработки	62
2.6 Сравнение с проектами ЦВЦБ в других странах	67
<b>3. Экономические и регуляторные аспекты</b>	<b>71-88</b>
3.1 Экономические аспекты	71
3.2 Аспекты регулирования	81
3.3 Межбанковские платежи	87
3.4 Трансграничные платежи	88
<b>4. Следующие шаги</b>	<b>90-92</b>
Подход к изучению вопроса внедрения ЦТ	90
<b>Отзывы экспертов</b>	<b>93</b>
<b>Список литературы</b>	<b>95</b>

## Благодарность

Исследовательская работа по различным аспектам внедрения цифрового тенге проводится в тесном сотрудничестве с международными организациями и ведущими мировыми экспертами, изучающими цифровые валюты центральных банков.

Национальный Банк Республики Казахстан выражает благодарность за поддержку в проведении исследования международным партнерам и экспертному сообществу:



## Отзывы экспертов



«Доклад может служить ориентиром для других центральных банков, неправительственных организаций, ученых, энтузиастов цифровых- и криптовалют и вообще всех, кто просто хочет получить представление о том, как ЦВЦБ может быть внедрена».

### Профессор Джамиэль Шейх

Основатель CBDC Think Tank,  
профессор Колумбийского Университета



«Я выражаю благодарность НБРК за подготовку этого превосходного отчета. В документе содержатся ответы на такие важные вопросы, как последствия регулирования, применение DLT для снижения риска узловых точек отказа и применение программируемости».

### Вилли Лим

Руководитель направления  
стратегического консалтинга в сфере  
цифровых валют и платежей, R3

# Резюме

В настоящем документе представлены результаты первой стадии пилотного проекта по внедрению национальной цифровой валюты Республики Казахстан. Проект стартовал в 2021 году и был реализован Национальным Банком Республики Казахстан при тесном сотрудничестве с участниками финансового рынка, экспертным сообществом и международными партнерами.

Цифровой тенге выступит третьей формой национальной валюты Казахстана наряду с наличными и безналичными деньгами, станет дополнительным платежным инструментом для участников делового оборота, обеспеченным обязательствами НБРК.

Ключевой мотивацией в изучении цифрового тенге служит его потенциал в улучшении финансовой инклюзивности, развитии конкуренции и инноваций в индустрии платежей, а также повышении конкурентоспособности финансового сектора Казахстана на глобальном рынке.

Основными целями пилотного проекта на 2021 год являлись проверка жизнеспособности концепции ЦТ через экспериментальное подтверждение его технологической реализуемости розничной платформы на базе технологии распределенного реестра, а также определение основных параметров модели ЦВЦБ для Казахстана совместно со всеми заинтересованными сторонами.

В рамках пилотного проекта были реализованы базовые сценарии жизненного цикла ЦТ – от эмиссии и распределения до покупок и переводов с использованием ЦТ. Среди достигнутых преимуществ реализованного технологического решения можно выделить:

- токенизация права собственности – ЦТ хранится у пользователя в виде токенов в цифровом кошельке на его мобильном устройстве (или другом носителе), что позволяет обеспечить полный контроль за деньгами
- платежи в оффлайн-режиме - пользователи ЦТ могут совершать покупки при отсутствии доступа в интернет как у самого клиента, так и у продавца

- настраиваемая анонимность - детали транзакций могут быть скрыты от всех участников расчетов (в том числе по выбору пользователя) при обеспечении возможности проведения необходимых проверок
- токены специального назначения – программируемость ЦТ позволяет закладывать ограничения на траты в структуру токена и упрощать отслеживание целевого использования
- простота интеграции – инфраструктура ЦТ предоставляет возможность легкого подключения и реализации собственных сценариев использования для традиционных (БВУ) и новых (финтех) игроков финансового рынка.

В реализации учитывался международный опыт других центральных банков, существенно продвинувшихся в создании токенизированных розничных цифровых валют, а также экспертиза технологического партнера пилотного проекта - компании Accenture, обладающей передовым опытом реализации проектов в области цифровых валют в Швеции, Сингапуре, Канаде, Еврорегии, США, Швейцарии, ЮАР и других странах.

По итогам проекта были подтверждены гипотезы о технологической реализуемости концепции ЦТ и был определен перечень вопросов и задач для дальнейшей проработки. Кроме того, была выработана первичная модель оценки влияния ЦТ на экономику, финансовую стабильность и денежно-кредитную политику, а также возможные подходы к регулированию.

Модель принятия решения о необходимости внедрения цифровой валюты будет определена в июле 2022 года. Приоритетом НБРК в выработке решения будет являться итоговый эффект для потребителей платежных услуг.

Решение о необходимости внедрения ЦТ будет принято в конце 2022 года по результатам всестороннего исследования потенциальных выгод и рисков, проработки технологических аспектов, влияния на денежно-кредитную политику и финансовую стабильность, а также эффекта для Национальной платежной системы и ее участников.



## Введение

Настоящий доклад является результатом исследования НБРК о потенциале, преимуществах и рисках, организационных и технологических возможностях внедрения и использования цифровой валюты центрального банка в Республике Казахстан.

Целью доклада является информирование широкой публики, профессиональных участников рынка и финансового сообщества о ключевых результатах пилотного проекта, новых функциональных возможностях ЦТ, а также экономических аспектах внедрения ЦТ.

### Ключевые вехи пилотного проекта в 2021 году.

- в мае опубликован консультативный доклад для публичных обсуждений [«Цифровой Тенге»](#)
- с мая по декабрь проведена серия профильных встреч и обсуждение с участниками рынка, экспертным сообществом, государственными органами, а также международными партнерами
- в июне стартовал пилотный проект для оценки технической реализуемости ЦТ, в рамках которого был реализован прототип платформы, а также протестирован ряд сценариев с подключением внешних участников с участием двух банков
- в сентябре проведены опросы и интервью с участниками рынка для уточнения приоритетов и потребностей в развитии новых платежных инструментов
- в ноябре в рамках IX Конгресса Финансистов Казахстана были презентованы предварительные результаты пилотного проекта
- в декабре был подготовлен текущий доклад об итогах пилотного проекта.

### Настоящий доклад состоит из четырех ключевых разделов.

- в первой части обозначены предпосылки появления ЦВЦБ, их особенности и преимущества, а также ключевые характеристики ЦТ в контексте Национальной платежной системы Казахстана
- во второй части документа раскрываются основные результаты пилотного проекта по оценке технологической реализуемости концепции ЦТ, включая описание выбранного подхода, реализованных сценариев, ключевых архитектурных решений и аспектов для дальнейшей проработки
- в третьей части доклада описаны результаты исследования экономических и регуляторных аспектов внедрения ЦТ
- в четвертой части очерчен подход и дальнейшие шаги по проработке вопроса внедрения ЦТ в Казахстане.



МАЙ

**5 мая** публикация доклада, приглашения на 12 мая  
**12 мая** обсуждение с рынком  
**31 мая** публикация и рассылка ответов на вопросы участников обсуждения

ИЮН

**15-29 июня** обсуждения с другими ЦБ в рамках CBDC Think Tank  
 обсуждения с IMF

ИЮЛ

**14 июля** отправка приглашения на профильную встречу через АФК с презентацией, где указаны требования для присоединения к пилоту  
**16 июля** обсуждение с ЦБ Венгрии  
**23 июля** профильная встреча с БВУ, приглашение в пилот  
 обсуждения с WEF

АВГ

**3 августа** получение от АФК списка БВУ, желающих присоединиться к пилоту  
**5-12 августа** рабочие обсуждения с БВУ по вопросам участия в пилоте  
**24 июля-12 августа** разъяснение требований для БВУ  
**24 августа** отправка приглашения БВУ на профильную встречу 27 августа  
**27 августа** профильная встреча с БВУ, рассылка презентации, приглашение на интервью и следующую профильную встречу 17 сентября  
**3 августа** обсуждение ЦВЦБ Китая в рамках CBDC Think Tank  
 обсуждения с IMF

СЕН

**2-15 сентября** онлайн-опрос БВУ  
**6-14 сентября** проведение интервью с БВУ  
**17 сентября** профильная встреча с БВУ, презентация ответов на вопросы БВУ, консолидированных во время интервью  
**9 сентября** Global CBDC Challenge Masterclass Singapore Fintech Festival

ОКТ

**4-6 октября** CBDC academy Lighthouse Communications LLC  
**6 октября** BIS Conference FSI-IOSCO  
**21 октября** обсуждение с ЦБ Швеции  
 обсуждения с BIS, IMF

НОЯ

**12 ноября** проведение пленарной сессии в рамках IX Конгресса финансистов с участием представителей Accenture, R3, IMF, WEF  
**23 ноября** обсуждение ЦВЦБ проекта Норвегии в рамках CBDC Think Tank  
 обсуждения с IMF

ДЕК

**15 декабря** публикация итогового доклада



# Предпосылки и развитие ЦВЦБ в Казахстане

стр. **10-23**

### Формирование функции денег

Изначально деньги были представлены в материальной форме: от всевозможных ценных вещей до слитков и монет из драгоценных металлов или других практичных в использовании материалов. На начальном этапе деньги выполняли функцию средства обращения и меры учета, позволившую преодолеть ловушку «двойного совпадения потребностей» бартерного обмена.

Появление банковского дела закрепило следующую важную функцию денег – служить средством сохранения и накопления материальной ценности. С целью удобства хранения и расчетов банки начали выпускать собственные валюты, стоимость которых обычно обеспечивалась материальными ценностями, хранящимися в банке. При этом было невозможно достоверно проверить соответствие между стоимостью валюты и средствами в хранилище банка. Использование средств зависело от уровня доверия к их эмитенту: готовность принимать определенную валюту определялась доверием конкретного человека к конкретному банку.

Желание иметь универсальное платежное средство, не зависящее от действий частных финансовых организаций, привело к появлению фиатных денег, чья ценность состоит в доверии к выпустившему их государству и гарантируется центральным банком.

### Цифровизация

Прогресс компьютерных технологий способствовал дальнейшему развитию банковских услуг и привел к появлению электронных платежей и безналичной формы денег.

Новой вехой развития финансовых рынков стало возникновение в начале XXI века криптовалют. Благодаря появлению следующего поколения технологий появилась принципиальная возможность передачи ценности цифровым способом без финансового посредничества традиционных финансовых институтов и двойного расходования. Однако несмотря на технологические преимущества криптовалют, их рыночная капитализация подвержена значительным колебаниям, ценообразование недостаточно прозрачно, а юридический статус остается неопределенным, что ограничивает возможности их применения в качестве платежного средства.

Криптовалюта – цифровой актив на основе технологии распределенного реестра (DLT) и блокчейна. Криптовалюты не имеют единого эмитента: их эмиссия является децентрализованной.

Часть этих проблем смогли решить стейблкоины, обладающие искусственно фиксированным курсом. Однако по своей природе стейблкоины остаются частными, не подкрепленными официальным статусом активами.

## 1.1 Исторические предпосылки и тренды в платежной индустрии

Стейблкоины – криптовалюты, стоимость которых привязана к стоимости другого, более стабильного актива, обычно к курсу какой-либо государственной валюты через обеспечение ликвидностью или алгоритмическим образом.

Развитие рынка криптовалют привело к возникновению новой экосистемы распределенных финансов – Decentralized Finance (DeFi). DeFi не полагается на финансовое посредничество традиционных финансовых институтов, используя блокчейн и смарт-контракты для оказания финансовых услуг. Преимущества, часто упоминаемые в контексте DeFi: демократизация, повышение доступности, гибкости и сложности финансовых транзакций – вместе с тем, создают высокие риски для финансово неподготовленных граждан и могут приводить к потере значительной доли сбережений.

В ответ на эти риски и вызовы центральные банки по всему миру начали исследования возможности создания собственных цифровых валют, которые совместят традиционные функции денег с технологическими запросами современной цифровой экономики таким образом, чтобы это удовлетворяло интересам и потребностям всех экономических участников.

Тематический квартальный обзор Банка международных расчетов, опубликованный в апреле 2021 года, зафиксировал 65 исследовательских проектов ЦВЦБ по всему миру, а обновление обзора в октябре этого же года упоминает уже о 84 проектах. Количество пилотных проектов за этот период увеличилось с 9 до 26 [\[26\]](#).

## 1.2 ЦВЦБ в сравнении с другими формами денег

ЦВЦБ – цифровой платежный инструмент и обязательство центрального банка. Являясь носителем ценности и платежным инструментом ЦВЦБ на основе токена представляет собой третью форму национальной валюты. ЦВЦБ совмещает ряд свойств наличных и безналичных денег, при этом дополняя их новыми функциональными возможностями для участников делового оборота и государственных институтов.

### 1. ЦВЦБ и наличные средства

Преимущества расчетов наличными формами денег:

- ✓ являются обязательством центрального банка
- ✓ простота (при передаче купюры из рук покупателя в руки продавца перевод денежной ценности происходит мгновенно и окончательно без финансового посредничества и последующих расчетов)
- ✓ анонимность (продавцу и покупателю нет необходимости знать друг о друге какую-либо дополнительную информацию, например, номер банковского счета или мобильного телефона)
- ✓ расчеты без подключения к Интернету.

Однако преимущества наличных становятся их недостатками в иных ситуациях:

- ✓ неудобство использования бумажных купюр в расчетах (размен, отсутствие сдачи)
- ✓ отсутствие возможности совершить платеж на расстоянии
- ✓ риски утери, кражи, порчи, износа, подделки
- ✓ возможности для использования в незаконной деятельности за счет анонимности
- ✓ существенные издержки для бизнеса, коммерческих банков и центрального банка на выпуск, обращение и инкассацию.

Очевидные преимущества наличных (мгновенность и простота расчетов, анонимность, оффлайн-возможности) также применимы для ЦВЦБ. При этом, являясь электронной формой денег, ЦВЦБ по умолчанию не будет иметь вышеперечисленных рисков и ограничений, связанных с материальной природой наличных.

### 2. ЦВЦБ и безналичные средства

Сущность безналичных платежей заключается в том, что при осуществлении оплаты происходит обмен электронными сообщениями: списание средств со счета покупателя и их поступление на счет продавца.

## 1.2 ЦВЦБ в сравнении с другими формами денег

К преимуществам безналичных платежей относятся:

- ✓ возможность платежей без физического контакта, в том числе удаленно
- ✓ удобство хранения и доступа к средствам в цифровом формате
- ✓ удобство проведения платежей, включая возможность бесшовного встраивания оплаты в цифровой пользовательский опыт на цифровых платформах и доступ к платежам и переводам через мобильные приложения банков
- ✓ дополнительные сервисы и услуги, привязанные к платежам (доступ к выставленным счетам, автоплатежи, программы лояльности и бонусные программы, аналитика и управление финансами).

Однако у безналичных платежей есть и свои ограничения:

- ✓ требования по идентификации клиентов и невозможность осуществления анонимных транзакций
- ✓ отсутствие возможности проведения платежей при отсутствии интернет-связи (в том числе, например, в случае перебоев в подключении к сети, электроснабжении или т.п.)
- ✓ риски финансовых посредников, обеспечивающих проведение платежей и хранение средств клиента на счете (как обязательства коммерческой организации)
- ✓ отложенная финализация расчетов, например, для платежей через межбанковскую инфраструктуру розничных нетто-расчетов
- ✓ издержки на комиссии финансовых посредников, например при эквайринге платежей через карточную инфраструктуру.

ЦВЦБ сохраняют ряд преимуществ безналичных платежей: платежи без физического контакта, возможность проведения транзакций с помощью мобильного телефона, удобство хранения и доступа к средствам в цифровом формате, возможность бесшовного встраивания оплаты в пользовательский опыт (описание свойств ЦВЦБ и ЦТ см. далее разделы [1.3](#) и [2](#)).

Дополнительно к преимуществам безналичных платежей ЦВЦБ обеспечивают более высокий уровень анонимности (более подробно про анонимность – 2.4.2.6), поддерживают возможность проведения платежей в офлайн-режиме, переводятся между кошельками мгновенно и могут храниться непосредственно на устройствах пользователей (что обеспечивает гарантию полного контроля за средствами и их сохранность).



## 1.3 Преимущества и возможности ЦВЦБ

Внедрение ЦВЦБ потенциально принесет целый ряд совершенно новых цифровых возможностей и преимуществ, воспользоваться которыми смогут все ключевые группы стейкхолдеров: потребители, финансовые организации и государственные институты.

### Преимущества и возможности ЦВЦБ

#### ГРАЖДАНЕ



Удобство и простота использования «цифровых наличных» с гарантией ЦБ

Расширение доступности платежей (в т.ч. в удаленных регионах либо при временной недоступности интернета)

Снижение комиссий на платежи и переводы

Повышение безопасности и надежности платежей

#### БИЗНЕС



Сокращение затрат на работу с наличными и комиссии на транзакции

Оптимизация цикла расчетов, повышение скорости и эффективности

Снижение рисков

Новые сервисы и возможности для расчетов за счет программируемости и офлайн-платежей

#### ФИНАНСОВЫЕ ОРГАНИЗАЦИИ



Новые источники дохода, новые сервисы и услуги

Снижение издержек на инкассацию наличных

Снижение расчетных рисков и рисков партнерства

Оптимизация цикла расчетов

Снижение издержек на трансграничных платежах

#### ГОСУДАРСТВО



Повышения эффективности социальных и государственных платежей

Прозрачность и отслеживаемость государственных выплат

Развитие конкуренции

Повышение финансовой инклюзивности

Развитие инновационности финансового сектора

### ПРИМЕРЫ ПОТЕНЦИАЛЬНОГО ПРИМЕНЕНИЯ ЦВЦБ



#### Целевое использование

Токены специального назначения "Раскраска" токенов позволяет контролировать назначение платежей и отслеживать их использование



#### Платежи с участием государства

Уменьшение рисков ошибок, злоупотреблений, мошенничества, возможность контроля целевого использования, а также внесение быстрых изменений в параметры социальной помощи



#### IoT и M2M-платежи

ЦВЦБ будут удобным инструментом для реализации прямых (без посредников) платежей между устройствами интернет-вещей благодаря автономности и программируемости



#### Оплата по мере пользования (pay-per-use, pay-as-you-go)

Благодаря использованию смарт-контрактов ЦВЦБ обеспечит возможность оплаты за точное, фактически потребленное количество продуктов, ресурсов, услуг, предоставит необходимую гибкость, экономию и контроль за расходованием средств



#### Микроплатежи и списания на постоянной основе

Платежные свойства ЦВЦБ позволяют реализовать инкрементные платежи в моделях оплаты по мере пользования с бесконечно малым приращением, позволяя сократить сопутствующие временные издержки



#### Платежи в цепочках поставок

Программируемость и отслеживаемость ЦВЦБ позволяет реализовывать автоматические (в т.ч. по специальным условиям) и прозрачные для участников цепочки поставок расчеты, снижая риски и издержки, повышая уровень доверия участников цепочки



### 1. Предпосылки внедрения цифровой валюты в Казахстане

Предпосылки запуска проекта ЦТ были представлены в [Докладе](#) для общественных обсуждений.

- ✓ **Финансовая инклюзивность.** Необходимость повышения финансовой инклюзивности и доступности современных цифровых платежей для категории граждан и бизнеса с ограниченным доступом к современным платежным услугам.

В 2021 году доля безналичных в розничном обороте Казахстана достигла 77% [\[36\]](#). Однако, в силу неравномерной географической концентрации финансовых и платежных услуг значительная часть населения Казахстана, особенно в сельской и удаленной местности, по-прежнему имеет ограниченный доступ к финансовым услугам и банковской системе.

- ✓ **Эффективность платежной инфраструктуры.** Наличие потенциала для улучшения существующей платежной инфраструктуры. Технологические новации способствуют: расширению возможностей для проведения платежей в оффлайн-режиме; повышению анонимности и конфиденциальности транзакций; созданию возможности для широкой публики обладать цифровой валютой, которая являются прямым обязательством центрального банка; дальнейшему повышению бесперебойности национальной платежной системы, поскольку децентрализованная инфраструктура (на базе технологий распределенных реестров) за счет отсутствия центрального звена как единой точки отказа потенциально более устойчива к технологическим сбоям, а новые возможности оффлайн-платежей также делают платежную инфраструктуру более устойчивой к сбоям в связи или электроснабжении.
- ✓ **Совершенствование платежей с участием государства.** Задача повышения эффективности сценариев платежей с участием государства обусловлена активной ролью государства в национальном экономическом развитии и существенными государственными социальными обязательствами.
- ✓ **Цифровизация платежной инфраструктуры.** Необходимость повышения технологической адаптированности платежной инфраструктуры, связанная с увеличивающимся присутствием частных криптовалют и стейблкоинов в финансовом секторе, повышением международной конкуренции в сфере разработки государственных цифровых валют, растущей ролью международных технологических компаний в финансовом секторе и цифровых платежах.

Исходя из данных предпосылок и проблематики НБРК определил основные цели разработки собственной цифровой валюты:

- дальнейшее развитие национальной финансовой и платежной системы
- рост финансовой инклюзивности и доступности финансовых услуг
- повышение конкуренции в финансовом секторе и его конкурентоспособности
- создание технологической платформы для дальнейшей цифровизации
- обеспечение бесперебойности Национальной платежной системы
- повышение эффективности платежей с участием государства.

## 2. Определение ЦТ

Цифровой тенге - это обязательство НБРК, эмитируемое в электронной форме и распространяемое в рамках двухуровневой финансовой архитектуры совместно с участниками рынка. Существует технологическая возможность представления ЦТ в форме счета или токена. ЦТ может быть использован для розничных (retail) и оптовых (wholesale) расчетов. В рамках пилотного проекта в 2021 году была протестирована токенизированная форма цифрового тенге для использования в розничных расчетах. Мотивация к выбору данного подхода описана в майском [Докладе](#) для публичных обсуждений.

### Ключевые характеристики ЦТ

#### КОМБИНАЦИЯ СВОЙСТВ ДЕНЕГ ДЛЯ НОВЫХ ВОЗМОЖНОСТЕЙ



#### ОПРЕДЕЛЕНИЕ

Третья форма  
фиатных денег

Обязательство  
НБРК

Обменный курс  
1:1

#### СВОЙСТВА

Доступ на основе  
токена

Гибридная  
архитектура

Двухуровневая  
модель

#### ТРЕБОВАНИЯ К ПЛАТЕЖНОЙ СИСТЕМЕ

- ✓ Доступность 24/7
- ✓ Надежность
- ✓ Безопасность
- ✓ Гибкость
- ✓ Мгновенность
- ✓ Конфиденциальность
- ✓ Интероперабельность
- ✓ Масштабируемость

### 3. Новые возможности ЦТ для Национальной платежной системы Казахстана

ЦТ может стать дополнительным платежным средством РК. При этом платформа ЦТ обеспечит инфраструктуру для проведения платежей и переводов в ЦТ наряду с уже существующими платежными системами РК для безналичных расчетов. При проработке подхода к внедрению ЦТ важно учитывать характеристики и особенности существующих розничных и межбанковских платежных систем и отличия от предполагаемых свойств и характеристик платформы ЦТ.

Национальные Межбанковская система переводов денег (МСПД) и Система межбанковского клиринга (СМК) предоставляют базовую инфраструктуру для всех безналичных платежей в Казахстане, по итогам 2020 года:

- МСПД обеспечивает 90% B2B платежей банков и небанковских финансовых организаций, участников валютного рынка, рынка ценных бумаг;
- СМК обеспечивает более 63% от объема безналичных B2B платежей коммерческих банков и небанковских финансовых организаций [32].

В сфере розничных платежей необходимо выделить следующие важные платежные системы, используемые населением и бизнесом в Казахстане:

- международные платежные системы, обеспечивающие проведение карточных платежей;
- частные локальные платежные системы отдельных банков;
- национальная платежная система – Система мгновенных платежей.

ЦТ может дополнить действующую инфраструктуру розничных платежей через представление возможности создания новых платежных сервисов участниками рынка и возможности безналичного расчета в режиме оффлайн. При этом, в целевой платформе ЦТ будет обеспечена интероперабельность с существующей платежной инфраструктурой.

#### Карточные платежи в Казахстане

Карточные платежные системы в Казахстане представлены в основном картами, выпускаемыми и принимаемыми к оплате коммерческими банками в партнерстве с двумя ключевыми международными карточными схемами – Visa и Mastercard (зарегистрированы и функционируют также другие международные карточные системы, такие как American Express, Diners Club, UnionPay, Мир) [32]. Карточные платежи и переводы представляют собой удобный инструмент безналичных платежей и покрывают широкий спектр потребностей граждан и бизнеса.

### Динамика выпуска и использования платежных карт в Казахстане, млн шт.



по данным НБРК на 10.12.2021 [\[32\]](#)

Количество карточных транзакций (к которым относятся как транзакции по картам международных карточных схем, так и внутри локальных банковских систем) увеличилось с 232 млн в 2017 году до 2,88 млрд в 2020 году. Денежный объем этих транзакций вырос с 3 трлн тенге до 35,3 трлн тенге за тот же период [\[33\]](#).

Средняя сумма транзакций сократилась незначительно: с 13,1 тыс. тенге в 2017 году до 12,3 тыс. тенге в 2020 году. Это говорит о дальнейшем развитии карточных платежей, несмотря на инфляцию [\[33\]](#).

#### Локальные банковские платежные системы

К локальным банковским платежным системам в Казахстане относятся банковские системы, обеспечивающие платеж или перевод внутри экосистемы банков. Такие платежные системы являются замкнутыми, поскольку используют тот или иной вариант on-us-транзакций, когда и иницилирующая, и принимающая платеж стороны являются клиентами одного банка.

Количество и объем безналичных транзакций внутри локальных систем резко выросли в последние годы с 27 млрд тенге и 30 тыс. транзакций в 2017 году до 25,6 трлн тенге и 1,98 млрд транзакций в 2020 году [\[33\]](#).

Важно отметить, что транзакции внутри локальных систем более чем в два раза превышают транзакции по картам международных карточных схем, как по количеству, так и по объемам.

Так, в 2020 году в сравнении с вышеупомянутыми 1,98 млрд транзакций на сумму 25,6 трлн тенге, совершенных внутри локальных банковских систем, через международные карточные системы было проведено 899 млн транзакций объемом 9,7 трлн тенге [\[33\]](#).

### Сравнение объемов транзакций по международным и локальным платежным системам

		2016	2017	2018	2019	2020	10 мес. 2021
Количество транзакций, млрд транзакций	через международные платежные системы	0,12	0,23	0,52	0,85	0,90	0,94
	через локальные платежные системы	0,00	0,00	0,00	0,35	1,98	4,1
Объем транзакций, трлн тенге	через международные платежные системы	1,6	3,0	6,3	9,1	9,7	11,9
	через локальные платежные системы	0,1	0,0	0,0	4,9	25,6	45,8

по данным НБРК на 10.12.2021 [\[34, 35\]](#)

### СМП

Система мгновенных платежей предоставляет инфраструктуру для проведения межбанковских розничных мгновенных платежей и переводов [\[34\]](#). Достоинствами системы являются доступность и скорость транзакций для конечных пользователей, ограничением – зависимостью от участия в ней банков.

Диверсифицированный ландшафт платежной инфраструктуры на рынке Казахстана и динамичный рост объема безналичных операций демонстрируют возможности для развития новых платежных инструментов и дальнейшей цифровизации платежей. ЦТ может успешно дополнить существующие платежные системы РК, предоставляя пользователям дополнительную функциональность и платежные инструменты и создавая условия для конкурентного развития финансового рынка.

### 4. Ключевые принципы внедрения

Основополагающие свойства ЦТ, сформулированные НБРК, согласуются с базовыми принципами ЦВЦБ, разработанными Банком международных расчетов [\[27\]](#):

#### Принцип 1: «Не навредить» монетарной и финансовой стабильности

При внедрении ЦТ будут приняты во внимание потребности всех участников казахстанской денежной системы. Новая форма денег будет способствовать достижению целей совершенствования финансовой инфраструктуры, не нанося вреда финансовой стабильности страны.

Возможные риски в отношении денежно-кредитной политики и финансовой стабильности, технологические сбои будут проанализированы и учтены при дальнейшей разработке ЦТ.

#### Принцип 2: Дополнение существующих форм денег

ЦТ создается не для того, чтобы конкурировать, а для того, чтобы дополнять существующие формы денег. Ни одна из существующих форм денег не будет намеренно ограничиваться в обращении. НБРК продолжит поставлять наличные деньги в соответствии с совокупным спросом.

#### Принцип 3: Повышение эффективности платежей и способствование инновациям

Внедрение технологических достижений является одним из ключевых факторов реализации ЦВЦБ. НБРК и все участники финансовой системы будут отдавать приоритет постоянным инновациям, способствующим повышению эффективности платежной системы.

Также дизайн ЦТ учитывает международные принципы, разработанные G7 (Саммит большой семерки) [\[28\]](#). Эти принципы государственной политики для розничных ЦВЦБ являются продолжением базовых принципов, выдвинутых Банком международных расчетов. Принципы G7 поделены на две категории:

1) основополагающие принципы для внедрения ЦВЦБ:

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



2) дополнительные возможности ЦВЦБ:

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

### 5. Вопросы для практического исследования

Для принятия взвешенного решения о внедрении ЦТ необходимо провести оценку практической реализуемости решения, которое отвечает целям и задачам внедрения ЦТ и при этом не противоречит ключевым принципам (см. выше).

С этой целью НБРК инициировал в 2021 г. разработку пилотного проекта ЦТ, в котором постарался проверить гипотезы, сформулированные на основании предшествующего исследования.

### Взаимосвязь существующих проблематик и гипотез

#### Предпосылки и проблематика

Высокая доля наличных в розничных платежах

Неравномерная географическая концентрация финансовых услуг

Недостаточная эффективность платежной инфраструктуры, дефицит межсистемного взаимодействия

Необеспеченная потребность населения в недорогих и быстрых розничных платежах

Существенные издержки населения и бизнеса при проведении безналичных платежей

Необходимость повышения технологической адаптированности платежной инфраструктуры

#### Задачи развития Национальной платежной системы

Эффективность межбанковских расчетов

Обслуживание потребностей цифровых платежей

Снижение совокупных издержек участников

Снижение использования наличных за счет новых технологий

Повсеместное внедрение розничных платежей

Условия для конкуренции на финансовом рынке

#### Цели разработки ЦТ

Обеспечение конкуренции на финансовом рынке внутри страны

Обеспечение конкурентоспособности финансового рынка РК

Рост проникновения безналичных платежей

Бесперебойность Национальной платежной системы

Эффективность платежей с участием государства

#### Подтвержденные гипотезы

- ✓ Снижение издержек создания денег
- ✓ Социальные платежи
- ✓ Простой доступ
- ✓ Программируемость
- ✓ Удобство транзакций
- ✓ Транзакции в оффлайне
- ✓ Безопасность транзакций
- ✓ Аналитика
- ✓ Снижение издержек обращения

### Перечень гипотез для проверки в рамках пилотного проекта

Гипотеза	Описание
<b>Простой доступ</b>	Механизм получения доступа к системе ЦТ по удобству и безопасности, как минимум, не уступает существующему механизму доступа к платежной инфраструктуре
<b>Удобство транзакций</b>	Механизмы оплаты ЦТ и перевода ЦТ по удобству использования и скорости расчетов, как минимум, не уступают существующим механизмам – наличным и безналичным, как максимум - являются более эффективными
<b>Безопасность транзакций</b>	Механизмы оплаты ЦТ и перевода ЦТ по конфиденциальности, информационной безопасности и требованиям ПОД/ФТ как минимум, не уступают существующим механизмам - наличным и безналичным, как максимум , являются более эффективными в сравнении с ними
<b>Снижение издержек создания</b>	Снижение издержек по времени и по затратам, по сравнению с механизмом эмиссии наличных
<b>Снижение издержек обращения</b>	Снижение операционных издержек, связанных с системным учетом средств на всех уровнях, – от уровня НБРК до цифровых кошельков физлиц и ТСП
<b>Социальные платежи</b>	Механизм обеспечения населения социальной помощью по скорости, удобству и возможности отслеживания специального назначения, как минимум, не уступает существующему механизму, как максимум, являются более эффективными
<b>Программируемость</b>	Программируемая природа ЦВЦБ позволяет осуществлять сценарии ранее недоступные для наличных и безналичных расчетов, в т.ч. оффлайн-транзакции, покупка с ограничением (целевое расходование, запрограммированное в структуру ЦТ) и другие сценарии (внешние участники) с использованием смарт-контрактов
<b>Оффлайн</b>	Реализация возможности проведения платежей при перебоях в работе интернета или в регионах с недостаточным интернет-проникновением
<b>Аналитика</b>	Возможность получения расширенных данных по операциям в ЦТ для анализа и моделирования макроэкономических показателей

# Результаты пилотного проекта

стр. **25-69**

В Докладе для публичных обсуждений «Цифровой тенге» [\[31\]](#) представлено описание выбора параметров дизайна ЦТ для пилотного проекта, ключевыми из которых являются:

Аспект дизайна	Описание
<b>Розничная валюта</b>	ЦТ является розничной цифровой валютой, доступной для широкого круга пользователей (физических и юридических лиц).
<b>Гибридная инфраструктура</b>	<p>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:</p> <ul style="list-style-type: none"> <li>▪ подключение инфраструктурных участников (БВУ, госучреждений и т.п.) к платформе обеспечивает НБРК</li> <li>▪ подключение физических и юридических лиц обеспечивают БВУ через открытие цифровых кошельков на платформе ЦТ, предоставляемой НБРК</li> <li>▪ отсутствие двойной траты, то есть невозможность использования одних и тех же ЦТ в разных операциях, гарантируемое НБРК</li> </ul>
<b>Доступ на основе токена</b>	При доступе на основе токена использование средств зависит от способности получателя платежа проверить действительность платежного объекта.
<b>Двухуровневая архитектура</b>	<p>НБРК осуществляет эмиссию цифровой валюты, контроль за безопасностью системы, отвечает за распределенный реестр и устанавливает критерии, которым должны соответствовать участники пилотной платформы.</p> <p>Посредники (коммерческие банки, финтех-организации) осуществляют взаимодействие с конечными пользователями: открытие и обслуживание кошельков клиентов, проведение розничных платежей, КУС.</p>

Разработка прототипа с указанными характеристиками позволяет ответить на вопросы выполнимости предположений об использовании технологии распределенного реестра для ЦВЦБ:

- ✓ Отслеживаемость транзакций участниками. Участники транзакций могут проверить достоверность полученных токенов по данным истории транзакций токена. Таким образом, обеспечиваются гарантии проверяемости и прослеживаемости происхождения токенов, что помогает выполнению требований ПОД/ФТ [\[6\]](#).

- ✓ Повышение надежности транзакций. В финансовых системах, основанных не на распределенных реестрах, данные могут храниться централизованно и несмотря на возможности репликации и резервирования данных, существует глобально единая точка отказа – инфраструктура определенного банка. В случае распределенных реестров у каждого участника транзакции сохраняется копия транзакции, а также история всех транзакций в самом переданном токене ЦТ. Такое децентрализованное хранение позволяет уменьшить риск потери или компрометации приватных данных [7].
- ✓ Возможности программируемости. Архитектура распределенных реестров позволяет создавать смарт-контракты, которые могут повысить скорость транзакций, автоматизируя некоторые платежи и переводы [6,7]. Подробнее возможности программируемости и их использование в пилотном проекте описаны в разделе [2.4.2.5](#).

Для проверки жизнеспособности концепции ЦТ было принято решение разработать прототип платформы ЦТ. Прототип позволяет проверить реализуемость ключевых платежных сценариев, а также оценить риски и ограничения, связанные с использованием технологии распределенного реестра и доступа на основе токена.



### Жизненный цикл и специальные решения, протестированные в пилотном проекте



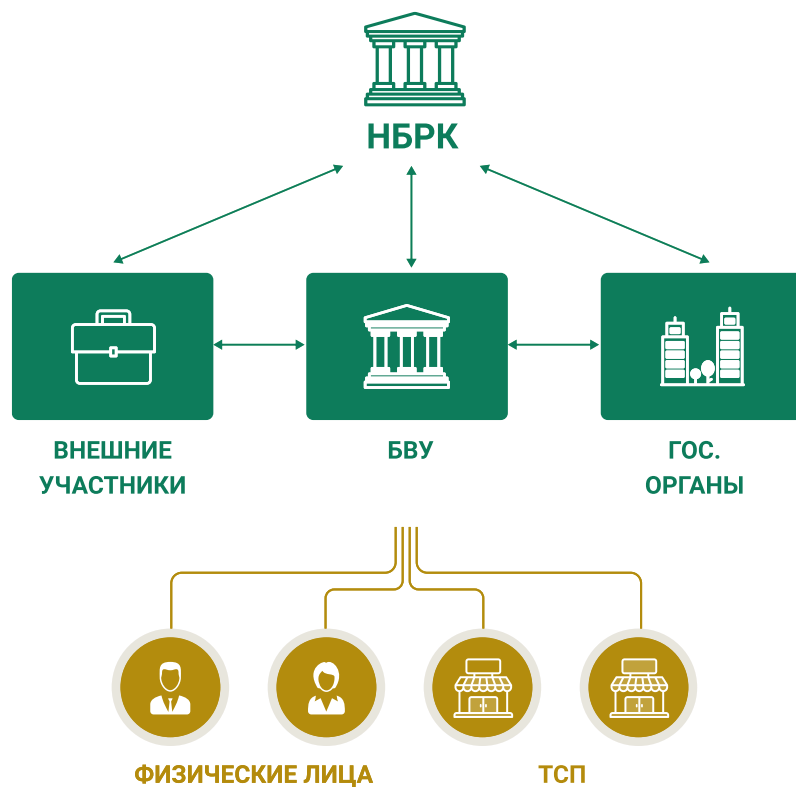
По результатам пилотного проекта были достигнуты следующие результаты:

1. Экспериментально подтверждена возможность реализации розничной ЦВЦБ на базе DLT-технологии.
2. Разработаны и протестированы ключевые сценарии жизненного цикла ЦВЦБ – от эмиссии до обращения.
3. Протестированы новые потенциальные преимущества, которые открывают ЦВЦБ для граждан и коммерческих организаций, в том числе: оффлайн-платежи, программируемость на уровне токена, гибкость системы в отношении баланса между анонимностью транзакций и ПОД/ФТ (настраиваемая анонимность).
4. Протестировано подключение БВУ и других внешних участников к инфраструктуре «ЦТ» (Более подробно – 2.4.2.9).

## 2.2 Роли, участники и архитектура пилотной платформы

Для возможности выполнения операций с ЦТ на пилотной платформе предусмотрены следующие участники, которые взаимодействуют между собой в соответствии с двухуровневой архитектурой:

### УЧАСТНИКИ ПИЛОТНОЙ ПЛАТФОРМЫ



### НБРК

НБРК является оператором пилотной платформы, обеспечивает подключение внешних участников к платформе, осуществляет эмиссию, распределение, погашение ЦТ и мониторинг работы платформы. Также НБРК является гарантом однократного использования токенов и их легитимности как платежного средства: в инфраструктуре НБРК размещена нотариальная нода распределенного реестра.

### Банки второго уровня (БВУ)

БВУ предоставляют пользователю цифровые кошельки для осуществления платежей с использованием ЦТ, отвечают за выполнение требований ПОД/ФТ и КУС, держат и распространяют токены, осуществляют обмен, погашение, восстановление ЦТ и межбанковские переводы.

## 2.2 Роли, участники и архитектура пилотной платформы

### Государственные органы

Государственные органы определяют специальное назначение токенов ЦТ, выполняют их распределение среди конечных пользователей, а также осуществляют контроль за целевым расходованием выданных денежных средств. Осуществление платежей происходит через БВУ.

### Торгово-сервисные предприятия (ТСП)

Торгово-сервисные предприятия осуществляют предоставление услуг и товаров физическим лицам, являются клиентами БВУ и открывают кошельки в БВУ, осуществляют онлайн- и оффлайн-транзакции с помощью токенов (покупка и перевод) с использованием электронных кошельков.

### Физические лица

Физические лица – граждане, которые являются пользователями платформы и осуществляют взаимодействие с ТСП, БВУ и внешними участниками. Физические лица управляют своими ЦТ с помощью электронных кошельков.

### Внешние участники

К внешним участникам относятся: финтех-компании; технологические компании, включая провайдеров IoT и других решений; регулируемые участники финансового рынка (провайдеры финансовых продуктов и сервисов).

Внешние участники подключаются к платформе и на ее базе создают дополнительные сервисы и продукты. Целью привлечения внешних участников является демонстрация возможностей платформы по построению бизнес-приложений и реализации дополнительных сценариев для создания экосистемы сервисов и продуктов ЦТ. Внешние участники подключаются к платформе через интеграционные сервисы БВУ для проведения транзакций с ЦТ и обмена ЦТ на фиатную валюту.

### Каждому из участников в пилотной платформе соответствует определенная роль:

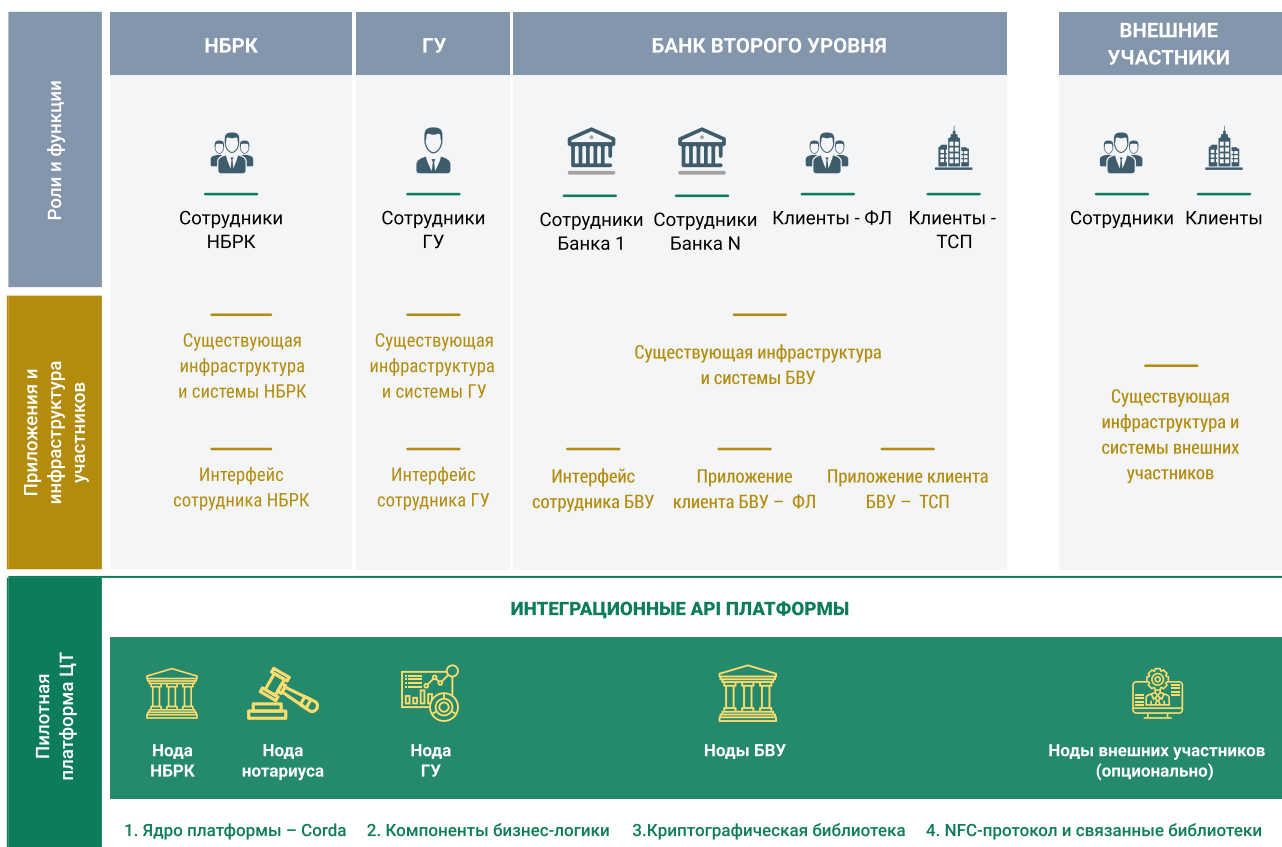
Участник	Роли на платформе
НБРК	Центральный банк (1 уровень)
БВУ	Инфраструктурные участники 2-го уровня
Государственные органы	Инфраструктурные участники 2-го уровня
Торгово-сервисные предприятия	Пользователи
Физические лица	Пользователи
Внешние участники	Участники экосистемы

## 2.2 Роли, участники и архитектура пилотной платформы

Для возможности тестирования сценариев жизненного цикла ЦТ в пилотной платформе, построенной на двухуровневой модели распределения ЦТ (рисунок далее), выполнена эмуляция следующих ролей:

- Центральный Банк (1-й уровень) – является нодой в сети ЦВЦБ, осуществляет функцию выпуска, погашения и перевода токенов.
- Инфраструктурные участники 2-го уровня (БВУ и государственные органы) – являются нодой в сети ЦВЦБ, могут взаимодействовать с 1-м уровнем и сами держать и распространять токены. В пилотном проекте были реализованы и протестированы внешние сценарии с двумя БВУ (см. раздел [2.4.2.9](#)). Внешние приложения БВУ-участников пилотного проекта подключены к пилотной платформе через пилотную реализацию API-платформы.
- Пользователи (физические лица и ТСП) – конечные пользователи, имеющие доступ к платформе через интерфейсы БВУ, в которых они обслуживаются. В пилотном проекте были разработаны демонстрационные приложения физических лиц и ТСП.

### Концептуальная архитектура пилотной платформы



## 2.3 Выбор технологического решения (DLT-платформы)

В качестве основы для реализации пилотного проекта по результатам сравнения разных технологий было выбрано решение на базе технологии распределенных реестров Corda от консорциума r3.

Ключевые критерии выбора:

Критерий	Описание
Тип лицензирования	Платформы с открытым исходным кодом
Контроль доступа к DLT-сети	Закрытый реестр, возможность организации контроля за доступом к сети новых участников
Безопасность и приватность	Возможность управления анонимностью, конфиденциальностью и отслеживаемостью транзакций
Гибкость и масштабируемость	Возможность масштабирования технологической платформы, ведения динамического реестра участников распределенного реестра
Производительность	Скорость обработки и выполнения транзакций в реестре
Интероперабельность	Поддержка ISO 20022 и иных стандартов

Для развития будущей экосистемы ЦТ важно наличие и гибкость функциональности достижения консенсуса, определения и управления правами доступа участников, а также возможность создания смарт-контрактов в реестре [8]. Платформа Corda предоставляет такие возможности [9].

Дополнительными критериями выбора в пользу Corda стал изначальный ориентир консорциума на разработку решений для финансовой отрасли, а также особый упор на конфиденциальность данных участников транзакций. Опыт успешного пилотирования ЦВЦБ на базе Corda уже имеют такие страны, как Швеция, Япония, Канада, Швейцария, а также Европейский Союз.



## 2.4 Сценарии пилотного проекта

ЦТ использует двухуровневую модель распределения. Это означает, что НБРК распределяет токены ЦТ на цифровые кошельки БВУ в обмен на безналичные средства участников. Конечные пользователи взаимодействуют с платформой ЦТ через БВУ. Подключение пользователей к платформе, пополнение кошельков и выполнение транзакций происходит именно через БВУ. В пилотном проекте банки предоставляют эти услуги через свои мобильные приложения.

### 1. Подход к определению списка тестируемых сценариев

Для оценки технологической реализуемости пилотной платформы было принято решение выполнить проверку предположений относительно того, как должна работать платформа (гипотезы) с помощью сформированных практических шагов (сценариев).

Учитывая перечень гипотез (таблица ниже), бизнес-требования к свойствам ЦТ, международный опыт реализации сценариев с ЦВЦБ, а также технологические особенности, был сформирован список приоритетных сценариев для тестирования в рамках пилотного проекта

### Соотношение сценариев и проверяемых в них гипотез

#	СЦЕНАРИЙ	ОПИСАНИЕ	Простой доступ	Удобство транзакций	Безопасность транзакции	Снижение издержек создания	Снижение издержек обращения	Социальные платежи	Программируемость	Оффлайн	Аналитика
1	Открытие кошельков инфраструктурных участников	Первоначальное создание электронных кошельков с ЦТ для инфраструктурных участников	☑								
2	Открытие кошельков клиентов БВУ	Первоначальное создание электронных кошельков с ЦТ для физических лиц	☑								
3	Эмиссия ЦТ	Первоначальное создание ЦТ без истории транзакций Эмиссия ЦТ на созданные кошельки участников				☑					
4	Распределение ЦТ	Реализация распределения ЦТ конечным пользователям через кошельки БВУ					☑				☑
5	Распределение ЦТ специального назначения	Реализация распределения целевых токенов конечным пользователям через БВУ					☑	☑	☑		☑
6	Онлайн-перевод	Перевод ЦТ между отправителем и получателем, физлица – клиенты разных банков при наличии интернет-соединения у всех участников		☑	☑		☑				
7	Покупка в режиме онлайн	Покупка физлицом товаров у ТСП за ЦТ при наличии интернет-соединения у физлица и ТСП. Физлицо и ТСП обслуживаются в разных банках		☑	☑		☑	☑			
8	Покупка в режиме оффлайн	Покупка физлицом товаров у ТСП за ЦТ при отсутствии интернет-соединения у физлица и ТСП. ТСП и физлицо обслуживаются в разных банках		☑	☑		☑	☑		☑	
9	Сценарии внешних участников	Сценарии внешних участников с использованием среды Пилотного Проекта для проверки и/или демонстрации технических возможностей	☑								

### 2. Реализованные сценарии

В данном разделе представлено описание сценариев, протестированных на пилотной платформе ЦТ.

#### ЦТ принадлежит пользователям

В текущих системах банковских платежей для получения клиентом Банка Б средств, отправленных клиентом Банка А, они должны пройти многоступенчатую процедуру взаиморасчетов.

С точки зрения процесса взаиморасчетов транзакции на платформе ЦТ гораздо более эффективны: так как ЦТ хранятся и передаются в токенах, их ценность можно передавать напрямую от отправителя к получателю без учета на балансах финансовых организаций. И хотя для соблюдения правил ПОД/ФТ и предотвращения двойной траты токенов сохраняются проверки со стороны БВУ и нотариальной ноды НБРК, исчезает необходимость проведения операций клиринга и реконсиляции. Благодаря этому процесс финализации транзакций и издержки сторон существенно сокращаются.

#### Транзакция в системе RTGS

#### Схема учета онлайн-перевода

##### Центральный Банк

АКТИВЫ	ПАССИВЫ
ВНЕ РАССМОТРЕНИЯ	Корр. Счет А 2 000
	Корр. Счет Б 3 000
	Корр. Счет А -50
	Корр. Счет Б +50

##### Банк А

АКТИВЫ	ПАССИВЫ
Корр. Счет А 2 000	Безнал. счет Алибека 500
Цифр. кошелек А 800	Другие клиенты 2 300
	Корр. Счет А -50

##### Банк Б

АКТИВЫ	ПАССИВЫ
Корр. счет Б 300	Безнал. счет ТСП 0
Цифр. кошелек Б 0	Другие клиенты 3 000
	Корр. Счет Б +50



- Ответственность за КУС и ПОД/ФТ
- Обязательство за ценность средств
- Передача ценности в транзакции

##### Центральный Банк

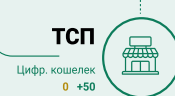
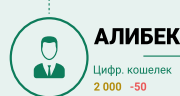
АКТИВЫ	ПАССИВЫ
ВНЕ РАССМОТРЕНИЯ	Корр. Счет А 1 950
	Корр. Счет Б 3 050
	Резервы под ЦВЦБ 1 000

##### Банк А

АКТИВЫ	ПАССИВЫ
Корр. Счет А 1 950	Безнал. счет Алибека 450
Цифр. кошелек А 800	Другие клиенты 2 300

##### Банк Б

АКТИВЫ	ПАССИВЫ
Корр. счет Б 3 050	Безнал. счет ТСП 50
Цифр. кошелек Банка Б 0	Другие клиенты 3 000



- Ответственность за КУС и ПОД/ФТ
- Обязательство за ценность средств
- Передача ценности в транзакции

Распределение ЦТ осуществляется согласно двухуровневой модели: НБРК пополняет цифровые кошельки БВУ в обмен на их безналичные средства. Дальнейшим взаимодействием с пользователями обеспечивают БВУ: подключение к платформе, пополнение кошельков и выполнение транзакций. В рамках пилотного проекта банки предоставляют эти сервисы через свои мобильные приложения.

### 2.1 Открытие кошельков инфраструктурных участников

Для работы с ЦТ БВУ и другие инфраструктурные участники должны подключить свои ноды к платформе и открыть кошельки, позволяющие проводить транзакции с токенами. Реализация возможности подключения новых участников к платформе подтверждает гипотезу доступности ЦТ для БВУ и других инфраструктурных участников.

**«Простой доступ»** – процесс открытия цифрового кошелька БВУ или иного инфраструктурного участника является как минимум таким же удобным и безопасным, как и существующий механизм доступа к платежной инфраструктуре.

В пилотной платформе процесс открытия кошельков инфраструктурных участников, генерации их адресов и подписей реализован с помощью функциональности платформы Corda.

### 2.2 Открытие кошельков клиентов БВУ

Открытие кошельков клиентов БВУ – это первоначальное создание электронных кошельков для клиентов БВУ. В пилотном проекте была протестирована такая возможность. В результате была подтверждена гипотеза удобства открытия кошелька клиента БВУ:

**«Простой доступ»** – по сравнению с открытием счетов в БВУ через мобильное приложение процесс открытия цифрового кошелька с ЦТ в БВУ является как минимум в такой же степени удобным и безопасным.

Платформа ЦТ построена по двухуровневой модели (раздел [2.2](#)). Подключение новых пользователей проводится исключительно через аккредитованные (участником первого уровня – НБРК) организации. На данный момент пилотируется доступ по схеме 1 к 1: один кошелек обслуживается одной организацией.

Физическое лицо или ТСП, желающее получить доступ к операциям с ЦТ, должно иметь доступ к мобильному приложению одного из БВУ. Сам процесс прохождения первичной идентификации пользователя со стороны банков, включая процедуры KYC, не входит в рамки данного проекта.

В приложении БВУ клиент может отправить запрос на открытие цифрового кошелька. Банк рассматривает заявку и подтверждает правомерность операции. В случае одобрения заявки на устройстве пользователя генерируется связка ключей, которые позволяют осуществлять транзакции на платформе ЦТ: онлайн-перевод, покупка в онлайн- и оффлайн-режимах.

### Мировой опыт

Возможные подходы, включая ограничения каждого из вариантов, рассматривались ранее центральным банком Швеции в отчете с результатами первой фазы пилотирования проекта e-krona [21].

В ЦТ использован подход, при котором и токены, и ключи хранятся на устройстве пользователя. Это позволяет бесшовно реализовать процесс оффлайн-покупки при внезапной потере связи на устройстве покупателя в отличие от подходов, где данная операция невозможна без предварительного сохранения части токенов на устройстве. При этом специальные механизмы хранения ключей клиентов БВУ (см. ниже) должны решить описанную банком Швеции проблему восстановления кошельков пользователей в случае утери устройства.

### Ключи и подписи

Для кошельков клиентов БВУ в платформе были реализованы специальные секретные ключи, которые гарантируют пользователям единоличный контроль над их средствами, при этом сохраняя для БВУ возможность отслеживать транзакции согласно требованиям ПОД/ФТ:

- ✓ Приватный ключ (`secretKey`) генерируется случайным образом. Известен только клиенту БВУ. После генерации разделяется на две части:
  - ключ просмотра (`viewKey`) – позволяет увидеть историю транзакций производимых с токенами пользователя. Хранится у БВУ, а также может быть передан другим организациям при согласии пользователя
  - операционный ключ (`spendKey`) – позволяет пользователю подписывать разрешение на передачу токенов. Хранится только у владельца кошелька
- ✓ Публичный ключ (`publicKey`). Публичный адрес кошелька клиента БВУ. Доступен клиенту БВУ, БВУ и другим участникам. Может быть зарегистрирован в общем реестре банков второго уровня, например, для возможности переводов ЦТ между клиентами по номеру телефона (сценарий «Онлайн-перевод» описан далее в разделе [2.5.3](#)).

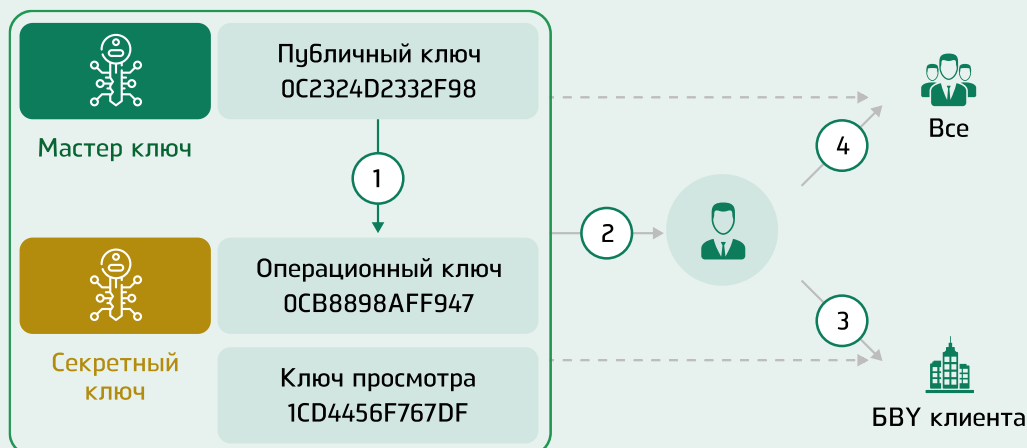
Схема генерации ключей представлена на рисунке далее:

1. При открытии кошелька пользователя на его устройстве генерируется публичный ключ. Из него формируются секретные ключи – операционный ключ и ключ просмотра
2. Клиент имеет доступ ко всем сгенерированным ключам

## 2.4 Сценарии пилотного проекта

3. Ключ просмотра передается в БВУ для соблюдения правил ПОД/ФТ
4. Публичный ключ является идентификатором клиента для получения платежей и доступен всем пользователям сети.

### Схема генерации ключей пользователя



## 2.3 Эмиссия ЦТ

Эмиссия – это первоначальное создание токенов ЦТ, которое производится в обмен на другие формы денег с разрешения НБРК.

Реализация данного сценария является необходимым базовым условием для любых других сценариев с использованием ЦТ и позволяет подтвердить важную гипотезу о преимуществах цифровой валюты:

**Снижение издержек создания** – по сравнению с наличными, эмиссия цифровой валюты, обеспеченной обязательствами НБРК, позволяет существенно сократить связанные расходы (а также косвенные издержки и негативное влияние на окружающую среду).

Инициатором запроса на эмиссию ЦТ может являться один из участников платформы – БВУ, государственный орган или НБРК в рамках реализации своих монетарных функций.

Любой токен содержит в себе информацию о своем эмитенте – НБРК Казахстана, которую невозможно подделать благодаря используемым криптографическим алгоритмам. Это позволяет всем участникам платформы однозначно определить подлинность токена. Процедура можно сравнить с идентификацией подлинности наличных средств с помощью анализа водяных знаков, заложенных при их печати.

### Ключевые свойства токена ЦТ

Ключевые свойства токена ЦТ:

- ✓ **Ценность.** Токен является символом определенной ценности, соответствующим количеству тенге, указанных в токене.
- ✓ **Проверяемость.** Ценность токена можно проверить на основании данных, имеющихся в самом токене.

Свойство «проверяемость» можно представить в виде шкалы. Слева расположены средства, чью ценность полностью гарантирует посредник: безналичные средства на банковском счете, чеки и пластиковые карты. Справа – средства, имеющие ценность сами по себе: золото, платина и т.д.



Токены ЦТ занимают промежуточное положение. Они не повторяют все свойства физических наличных денег. При этом по данным, которые содержатся в токене, можно проверить подлинность и ценность токена.

Эти свойства приближают токен ЦТ к характеристикам наличных средств.

Структура токена содержит:

- ✓ зашифрованную информацию о предыдущих владельцах, которая позволяет определить эмитента средств - НБРК
- ✓ информацию о текущем владельце ЦТ (в формате одноразового stealth-адреса)
- ✓ информацию о типе ЦТ (основной, специального назначения и т.п.)
- ✓ информацию о количестве ЦТ в скрытом виде



### 2.4 Распределение ЦТ

**Распределение ЦТ** – процесс передачи ЦТ от БВУ конечным пользователям, на цифровой кошелек (или потенциально другой носитель токенов) клиента.

Реализация данного сценария позволила подтвердить следующие гипотезы.

- **Снижение издержек обращения**

По сравнению с наличными средствами при распределении ЦТ отсутствуют издержки на транспортировку и хранение.

По сравнению с безналичными средствами: сокращение издержек, связанных с системным учетом средств на всех уровнях, так как средства на цифровом кошельке клиента не учитываются на балансе финансовой организации.

- **Аналитика.** Реализована возможность сбора данных по операциям в ЦТ для проведения анализа рынка и планирования макроэкономических показателей.

Клиент, который хочет получить ЦТ, направляет запрос в свой банк. После одобрения запроса банком, средства автоматически переходят с цифрового кошелька финансовой организации на счет кошелька клиента. Важным отличием от существующей системы безналичных платежей является окончательность перехода токенов: средства, находящиеся в кошельке клиента, по аналогии с наличными не учитываются на балансе финансовой организации.

### 2.5 Распределение ЦТ специального назначения

**Распределение ЦТ специального назначения** – процесс передачи специальных (целевых) токенов от государственного органа на счет цифрового кошелька клиента.

Реализация данного сценария позволила подтвердить следующие гипотезы:

- **Снижение издержек обращения**

По сравнению с наличными средствами при распределении тенге в цифровой форме отсутствуют издержки на транспортировку и хранение.

По сравнению с безналичными средствами будет наблюдаться сокращение издержек, связанных с системным учетом средств на всех уровнях, так как средства на цифровом кошельке клиента не учитываются на балансе финансовой организации и не требуют сверок или реконсильаций при учете.

- **Программируемость.** Функционал по ограничению целевого расходования средств обеспечивается типизацией токенов (то есть возможностью встроить в токен информацию о его типе, например, для отслеживания специального использования).

Изменение информации в структуре токена демонстрирует один из вариантов программируемости цифровых денег (также иногда упоминается как «маркировка» или «раскрашивание» денег).

- **Социальные платежи.** Ограничение расходования целевых средств достигается за счет особенности распределения этих средств, реализованной в пилотном проекте
- **Аналитика.** Реализована возможность сбора данных по операциям в ЦТ для проведения анализа рынка и планирования макроэкономических показателей.

### Описание сценария

Свойство программируемости ЦТ позволяет оптимизировать некоторые существующие платежные сценарии проще. Например, сценарий распределения денежных средств на определенные цели.

В качестве подтверждения программируемости токенов, на платформе ЦТ реализована типизация токенов и их распределение среди клиентов БВУ.

Банк первого уровня (НБРК) проводит эмиссию ЦТ общего типа. Далее участниками с соответствующими разрешениями возможна «типизация» полученных от НБРК цифровых денег. В пилотном проекте была реализована возможность маркировки эмитированных ЦТ одним из участников.

### Варианты программируемости ЦТ

ЦТ – это программируемое средство расчета:

Вариант 1. В токены ЦТ можно записать тип токена, данные его владельца или другие данные.

Вариант 2. В транзакциях – операциях с ЦТ можно скрывать определенные данные отправителя или получателя, то есть управлять анонимностью транзакций.

Вариант 3. На уровне распределенного реестра можно создать смарт-контракты, которые будут выполняться при создании транзакций с ЦТ.

При выполнении операций с ЦТ определенного типа может быть реализована проверка возможности операции. Для ЦТ специального назначения могут быть реализованы запреты на проведение некоторых операций. Например, в пилотном проекте был установлен запрет на выполнение «Онлайн-перевода», типизированного ЦТ клиентом. Также в случае попытки оплаты покупки в магазине ЦТ специального назначения, может проводиться проверка, вправе ли магазин принимать к оплате данные ЦТ.

Жизненный цикл ЦТ специального назначения в пилотной платформе изображен на рисунке далее.

### Жизненный цикл ЦТ специального назначения в пилотной платформе



◀ Безналичные средства на банковском счете

#### Выпуск



◀ Казначейство резервирует безналичные тенге в НБРК



◀ НБРК проводит эмиссию ЦТ

#### Распределение



◀ НБРК переводит ЦТ на цифровой кошелек ГУ



◀ На кошельке ГУ ЦТ приобретают свойства социальных



◀ ГУ переводит социальные ЦТ на цифровой кошелек БВУ



◀ БВУ переводит социальные ЦТ на цифровой кошелек физлица

#### Обращение



◀ Физлицо покупает товар у ТСП за социальные ЦТ



◀ На цифровом кошельке ТСП социальные ЦТ становятся обычными

#### Возврат



◀ ТСП обменивает ЦТ на безналичные тенге в БВУ



◀ БВУ обменивает ЦТ на безналичные тенге в НБРК

#### Погашение



◀ НБРК погашает ЦТ

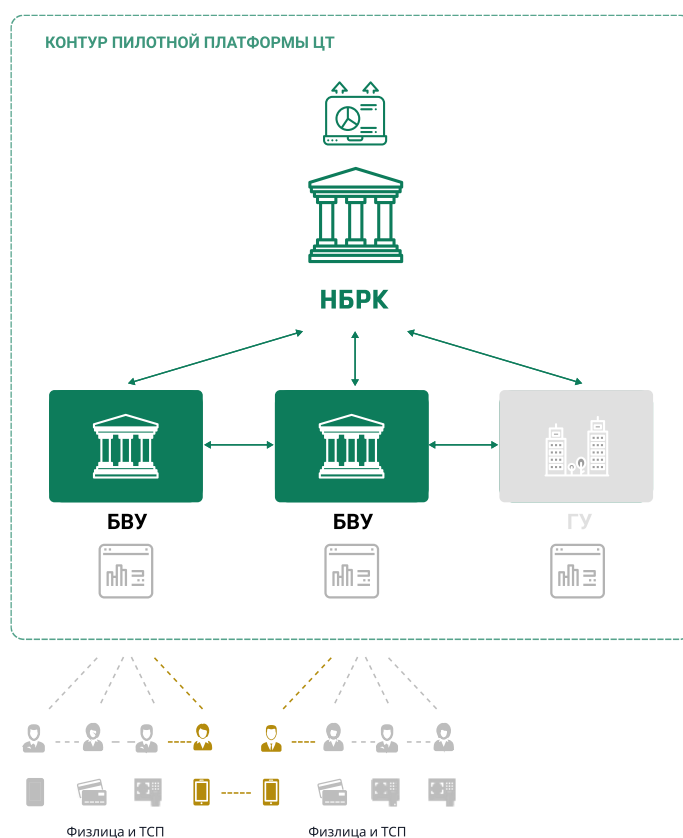
### 2.6 Онлайн-перевод

Онлайн-перевод – это передача токенов между кошельками клиентов в онлайн-режиме. Сценарий повторяет функциональность перевода средств между клиентами в безналичных платежных системах.

#### Протестированные гипотезы

- Удобство транзакций. Реализованный сценарий повторяет опыт онлайн-переводов, принятый в безналичных платежах, позволяя обеспечить как минимум, существующий тот же уровень удобства для пользователя.
- Безопасность транзакций. Токены позволяют однозначно установить эмитента средств, гарантируя их подлинность. При этом механизм консенсуса исключает возможность двойной траты токенов при наличии интернет соединения на устройствах участников.
- Снижение издержек обращения. Транзакции внутри распределенного реестра снижают риски и обязанности их участников. Это позволяет снизить стоимость транзакций благодаря реализации прямых транзакций без риска для её сторон.

#### Участники сценария «Онлайн перевод»



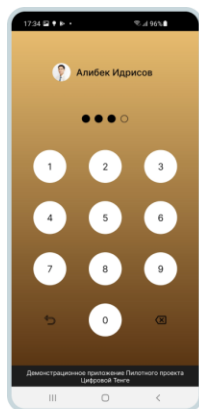
### Сценарий глазами пользователя

Процесс онлайн-перевода ЦТ в мобильном приложении БВУ показан на рисунке ниже. Для выполнения операции достаточно ввести номер телефона получателя и сумму перевода в мобильном приложении своего банка. После подписания транзакции клиентом и банками токены с ЦТ переводятся на цифровой кошелек получателя.

На уровне пользователя процедура может быть практически неотличима от современных решений безналичных онлайн-переводов. Однако при этом технология ЦТ не использует операции взаиморасчетов между финансовыми институтами – ценность передается напрямую между цифровыми кошельками клиентов. За счет этого значительно повышается эффективность: в случае традиционных централизованных систем безналичных платежей сдерживающим фактором является необходимость клиринга операций (а для карточной инфраструктуры отдельного цикла окончательных расчетов) для финализации расчетов.

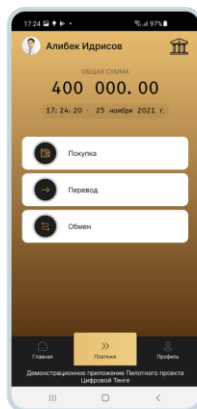
Для сохранения преимуществ наличных средств, в прототипе протестирована функция контроля анонимности со стороны пользователя: клиент в настройках своего «Профиля» может сам решить, хочет ли он, чтобы другие стороны транзакции видели его ФИО или предпочитает скрыть эти данные. Правда, речь не идет о скрытии информации от своей финансовой организации, иначе такое ограничение не позволит последним выполнять их основную функцию – ПОД/ФТ.

### Функциональное описание сценария «Онлайн - перевод»



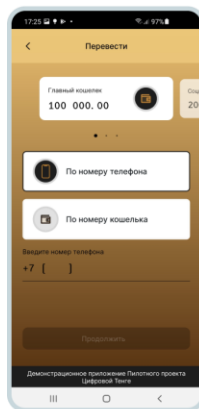
#### ШАГ 1

Алибек авторизуется в мобильном приложении Банка А



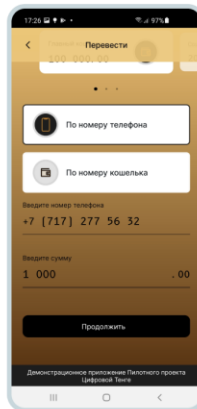
#### ШАГ 2

Алибек переходит в раздел «Платежи» и выбирает в меню «Перевод»



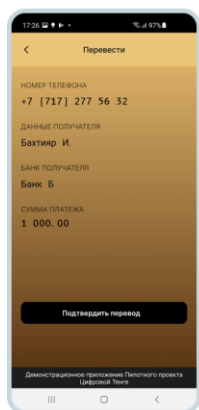
#### ШАГ 3

Алибек выбирает кошелек, с которого будет сделан перевод по номеру телефона: вводит номер Бахтияра



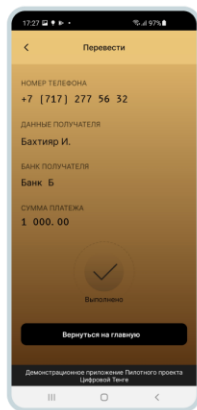
#### ШАГ 4

Алибек вводит сумму перевода



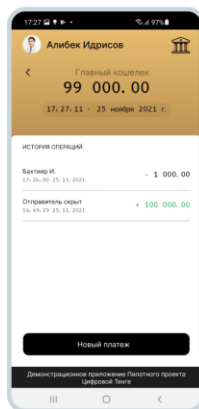
#### ШАГ 5

Алибек проверяет информацию о переводе и подписывает транзакцию



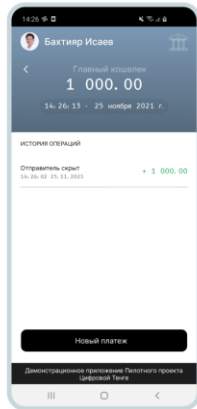
#### ШАГ 6

Алибек видит подтверждение успешности перевода



#### ШАГ 7

Алибек проверяет обновленный баланс в истории транзакций главного кошелька



#### ШАГ 8

Бахтияр видит поступление средств в истории транзакций главного кошелька



## 2.4 Сценарии пилотного проекта

### Учет средств при расчетах

(предварительный подход – будет дополнительно проработан на следующих этапах проекта)

Один из вариантов учета транзакций на платформе ЦТ, возможный благодаря выбранной модели доступа на основе токена, представлен ниже (по аналогии с наличными денежными средствами). При данном способе учета средства клиентов **не** учитываются на балансах их финансовых организаций. Это упрощает существующую систему взаиморасчетов между финансовыми организациями.

### Схема учета онлайн-перевода

#### НБРК

Активы				Пассивы			
Вне рассмотрения				Корр. счет Банка А	1950		
				Корр. счет Банка Б	3050		
				Счет ЦТ (резервы ЦТ)	1000		
Банк А				Алибек			
Активы		Пассивы		Активы		Пассивы	
Корр. счет в НБРК	1950	Безнал. счет Алибека	450	Безнал. счет	450	Вне рассмотрения	
Цифровой кошелек Банка А	800	Другие клиенты	2300	Цифровой кошелек Алибека	200 -50		
Банк Б				Бахтияр			
Активы		Пассивы		Активы		Пассивы	
Корр. счет в НБРК	3050	Безнал. счет Бахтияра	50	Безнал. счет	50	Вне рассмотрения	
Цифровой кошелек Банка Б	0	Другие клиенты	3000	Цифровой кошелек Бахтияра	0 +50		

### Мировой опыт

Модель на основе токена требует хранения в токене информации о предыдущих владельцах и транзакциях. Возможные подходы к разграничению информации, доступной новым владельцам токена, рассматривались ранее Центральным банком Швеции в рамках первой фазы пилотирования проекта e-krona [\[21\]](#). Пилот ЦТ решает данную проблему через криптографические механизмы сокрытия балансов (blinding keys) и адресов пользователей (stealth адрес), записанных в токене.

### Взгляд изнутри

#### Отслеживаемость транзакций

Владелец токенов с помощью своих ключей, зная публичный адрес другого участника, может создать транзакцию и подписать ее. Транзакция будет сформирована по правилам модели учета UTXO, приближенной к той, которая используется в безналичных транзакциях.

Основные свойства этой модели:

- ✓ у транзакции есть входящий и исходящий набор токенов
- ✓ набор входящих токенов транзакции клиента – это исходящий набор токенов предыдущей транзакции клиента
- ✓ токены с ЦТ передаются непосредственно от отправителя к получателю, поэтому при проведении транзакций не отражаются на балансах БВУ и НБРК.

Смысл транзакции, которую инициирует и подписывает клиент, может быть, например, таким:

Владельцем 30 тенге из этого токена теперь является участник с адресом a787803..

Эту транзакцию может просмотреть любой участник сети, равно как и увидеть входящий в нее токен. Из входящего токена также любой участник сети пользователь может получить публичный адрес владельца, его подпись и проверить соответствие этой подписи публичному ключу.

В долгосрочной перспективе историю транзакций с определенным адресом можно связать с конкретной организацией или клиентом. Таким образом возникает проблема отслеживаемости и деанонимизации транзакций.

В качестве решения в пилотной платформе используются одноразовые stealth-адреса, которые формируются из секретного и публичного ключей отправителя в момент проведения определенной транзакции.

В таком случае только пользователь, обладающий секретным ключом просмотра, может проверить принадлежность токена к данному публичному адресу. При этом проводить транзакции может только пользователь, владеющий операционной частью секретного ключа.

### Конфиденциальность

Благодаря применению stealth-адресов, идентификаторы участников не фигурируют в открытом виде. Однако при достаточном количестве транзакций, с помощью анализа сумм отправляемых токенов, третьи лица могут деанонимизировать участников и получить информацию о количестве ЦТ, которые остались у участников по результатам транзакций.

Corda предоставляет функциональность перевыпуска токенов для «разрыва» истории и решения подобной проблемы. Однако, на наш взгляд, это только частичное решение, так как разрыв истории даже после каждой транзакции не спасает от утечки информации о балансе отправителя [22].

На пилотной платформе входные и выходные данные транзакции модифицируются с помощью гомоморфных криптографических обязательств, чтобы скрыть балансы пользователей [4,5]. Таким образом владелец токена скрывает количество ЦТ в нем от внешних участников, при этом другие участники могут проверять валидность транзакций.

### Отсутствие интернета у получателя

Проблема использования криптографических обязательств в том, что для их формирования оба участника (и отправитель, и получатель) должны обменяться результатами некоторых вычислений при помощи секретных ключей. При этом получатель перевода должен находиться все время в онлайн-режиме, чтобы иметь возможность получать ЦТ.

Клиент-получатель иногда может находиться в оффлайн-режиме. Для того, чтобы он смог получать токены ЦТ по результатам входящих транзакций, обязательство по их подписанию может быть передано БВУ клиента, который всегда находится онлайн. Таким образом происходит разделение ролей «держателя» токенов с ЦТ (БВУ клиента) и «владельца» токенов (клиент).

Для реализации разделения функций «держателя» токенов и его «владельцев» секретный ключ можно разделить на две части, одну из которых будет использовать банк при обработке входящих транзакций по кошельку клиента.

В пилотном проекте для этого используются blinding keys – одноразовые ключи, которые скрывают количество ЦТ в токене и создаются для каждого токена в новой транзакции. С помощью таких ключей БВУ может участвовать в обмене для формирования корректного криптографического обязательства, но не может без участия клиента (владельца ЦТ и его секретных ключей для доказательства владения токеном – secretKey и viewKey) формировать новые транзакции или подменить сумму и получателя в транзакции.

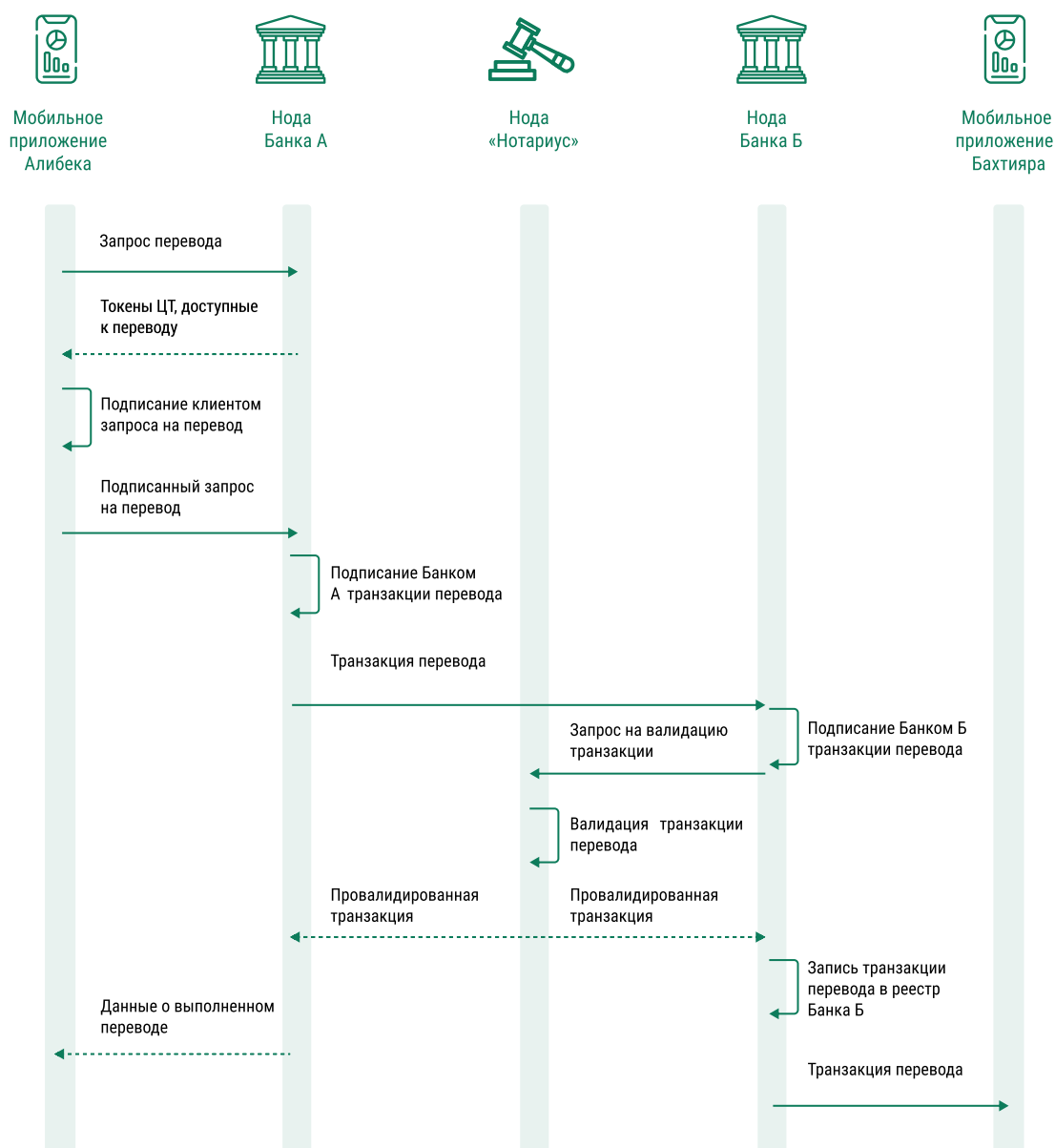
## 2.4 Сценарии пилотного проекта

Более подробно взаимодействие участников внутри платформы в случае сценария «Онлайн-перевода» представлено на следующем рисунке.

Помимо отправителя и получателя в транзакции принимают участие их банки и нотариальная нода НБРК. Нотариальная нода проверяет уникальность токенов подтверждая, что они не были потрачены ранее.

Банки выступают гарантом правомерности транзакций. При этом введение нескольких типов ключей оставляет за пользователем полный контроль над токенами, а криптографические механизмы позволяют ограничить информацию, доступную другим участникам, включая банк отправителя.

### Взаимодействие внутри платформы – онлайн-перевод



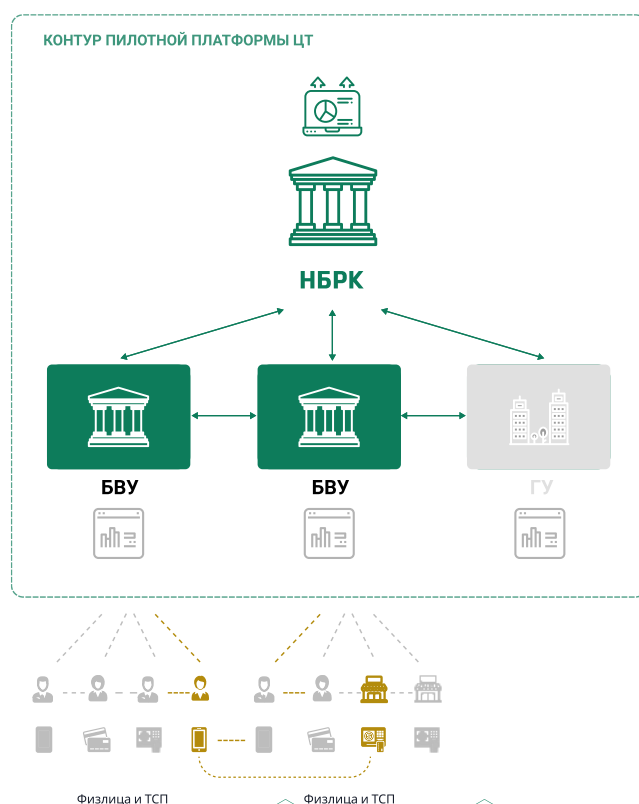
### 2.7 Покупка в режиме онлайн

Покупка в режиме онлайн – это перевод токенов между цифровыми кошельками на устройствах физического лица и ТСП при наличии интернет-соединения хотя бы у одного из участников. При этом во время проведения транзакции устройства пользователей должны находиться в пределах радиуса действия NFC-соединения или аналогичного протокола близкой коммуникации.

#### Протестированные гипотезы

- **Удобство транзакций.** Реализованный сценарий повторяет текущий опыт оплаты покупок в безналичных платежах, позволяя обеспечить как минимум тот же уровень удобства для пользователя.
- **Безопасность транзакций.** Токены позволяют однозначно установить эмитента средств, гарантируя их подлинность. При этом механизм консенсуса исключает возможность двойной траты токенов при наличии интернет-соединения на устройствах участников.
- **Снижение издержек обращения.** ЦТ позволяет производить низко рисковые транзакции с использованием средств под гарантией Национального Банка. Из-за модели учета на основе токенов расчеты являются окончательными в момент проведения транзакций. Это позволит снизить время расчетов и комиссии посредников.
- **Социальные платежи.** При покупке в режиме онлайн могут быть использованы специальные токены. Реализована возможность траты и проверки специальных токенов. Подход к ограничению трат по специальным токенам описан в разделе [2.4.2.5](#).

#### Участники сценария «Покупка в режиме онлайн»



### Сценарий глазами пользователя

Схема «Покупка в режиме онлайн», реализованная на пилотной платформе, представлена на рисунке далее. Для удобства пользователей механика процесса основана на опыте безналичных платежей: Кассир ТСП формирует заказ в своем приложении, выбирает ЦТ как способ оплаты и просит клиента поднести устройство. Покупатель заходит в приложение своего банка и выбирает цифровой кошелек, с которого будут списаны токены. При приближении устройств происходит обмен данными транзакции, и ЦТ поступает на счет ТСП.

Отметим, что оплата в данном случае произведена с социального кошелька. Это кошелек для работы с типизированными ЦТ, использование которых можно ограничить в определенных ТСП. Данный функционал возможен благодаря программируемости токена и не встречается в настоящее время в других открытых платежных системах.



### Функциональное описание сценария «Покупка в режиме онлайн»

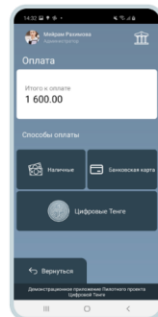
#### ШАГ 0

Алибек делает заказ в кафе и сообщает, что будет оплачивать ЦТ



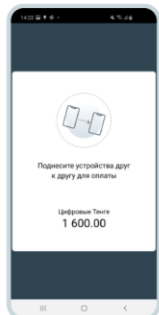
#### ШАГ 1

Кассир вводит заказ: выбирает товары из меню



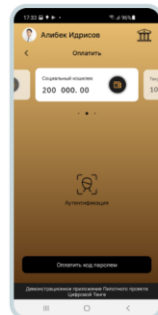
#### ШАГ 2

Кассир добавляет заказ в чек. Переходит в меню «Оплата» и выбирает способ оплаты: ЦТ



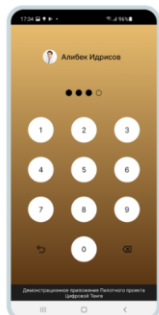
#### ШАГ 3

Кассир просит Алибека поднести устройство для оплаты



#### ШАГ 4

Алибек входит в приложение Банка А, нажимает «Покупка», выбирает соцкошелек



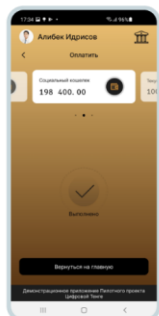
#### ШАГ 5

Алибек подтверждает разрешение на оплату через идентификацию



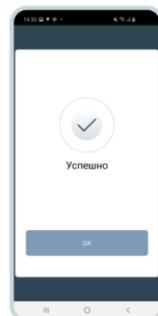
#### ШАГ 6

Алибек подносит телефон к устройству кассира



#### ШАГ 7

Алибек видит подтверждение оплаты и обновленный баланс соцкошелька



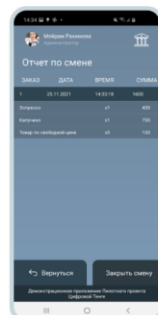
#### ШАГ 8

На устройстве кассира появляется информация об успешной продаже



#### ШАГ 9

Алибек проверяет списание средств в истории транзакций соцкошелька



#### ШАГ 10

Кассир переходит в раздел отчетов, где отражена транзакция продажи

### Взгляд изнутри

#### Методы передачи токенов

Для возможности передачи токенов с учетом всех использованных архитектурных решений (в частности, механизмов секретных ключей и сокрытия балансов) требуется обеспечить возможность двустороннего обмена между двумя устройствами.

Можно выделить три основные технологии обмена данными, которые удовлетворяют этому требованию:

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

Для проведения проверки технологической гипотезы в ходе пилотного проекта было принято решение использовать NFC-протокол и реализовать мобильные приложения с функциональностью проведения оффлайн-покупки для мобильных устройств на OS Android. Такой выбор среди иных возможных вариантов реализации был обоснован следующими факторами:

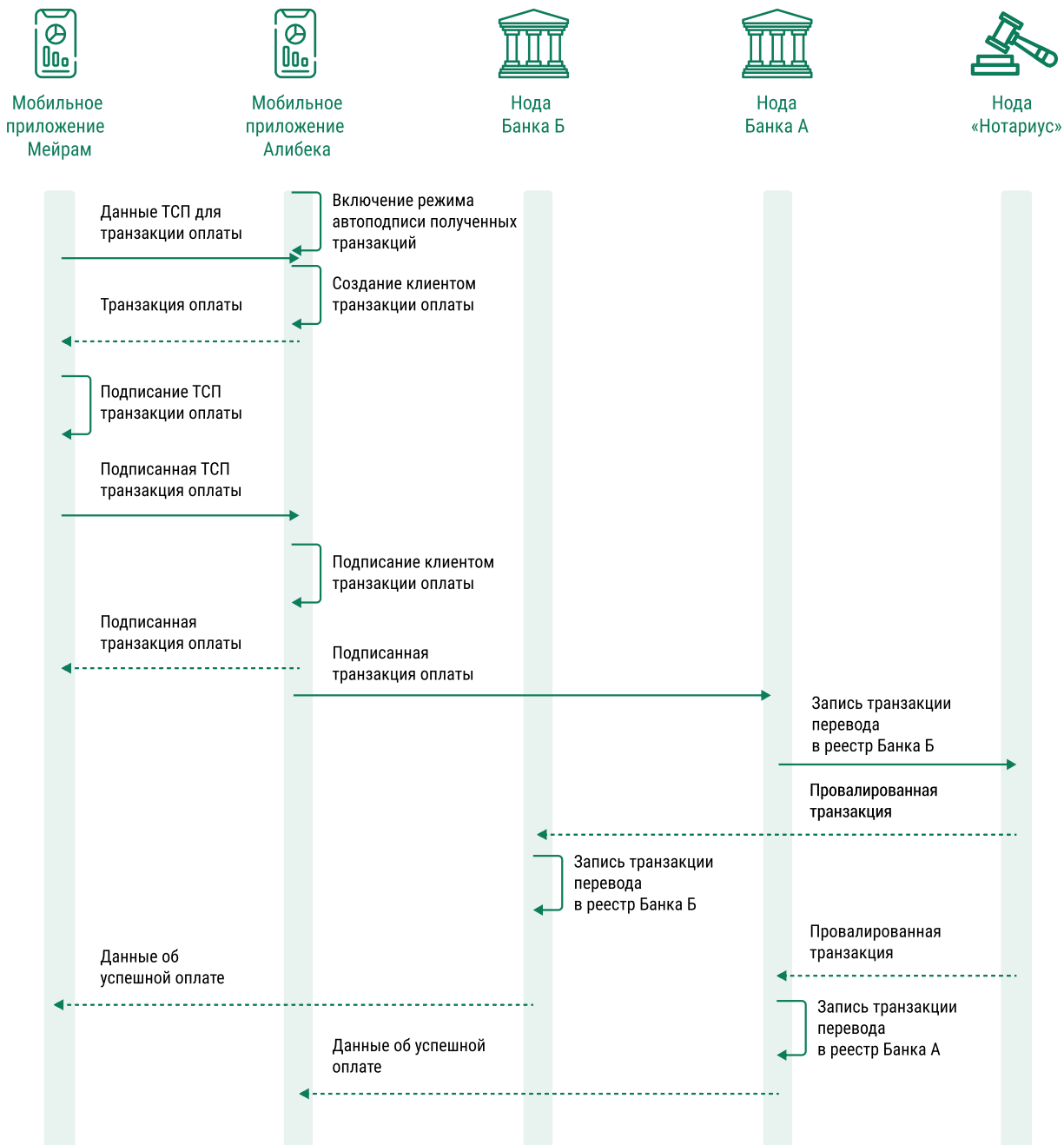
- механика работы с NFC-приложениями для оплаты покупок является нативной для пользователей, которые используют Apple Pay и Google Pay;
- реализация передачи и интерактивного обмена данными через NFC для Android является наиболее исследованной темой по сравнению с интерактивным обменом через NFC для iOS.

С технической точки зрения, главным отличием процесса покупки в режиме онлайн от онлайн-перевода является необходимость формирования шаблона транзакции и двустороннего обмена данными платежа непосредственно между устройствами участников.

Хотя сценарий оплаты покупки в режиме онлайн уже давно успешно используется для безналичной оплаты (карты МПС, ApplePay, SamsungPay и др.), при реализации подобных транзакций внутри DLT-платформы ЦТ возникает сложность, связанная с увеличением количества потоков и объема данных, передаваемых между устройствами участников.

## 2.4 Сценарии пилотного проекта

### Взаимодействие внутри платформы – покупка в режиме онлайн



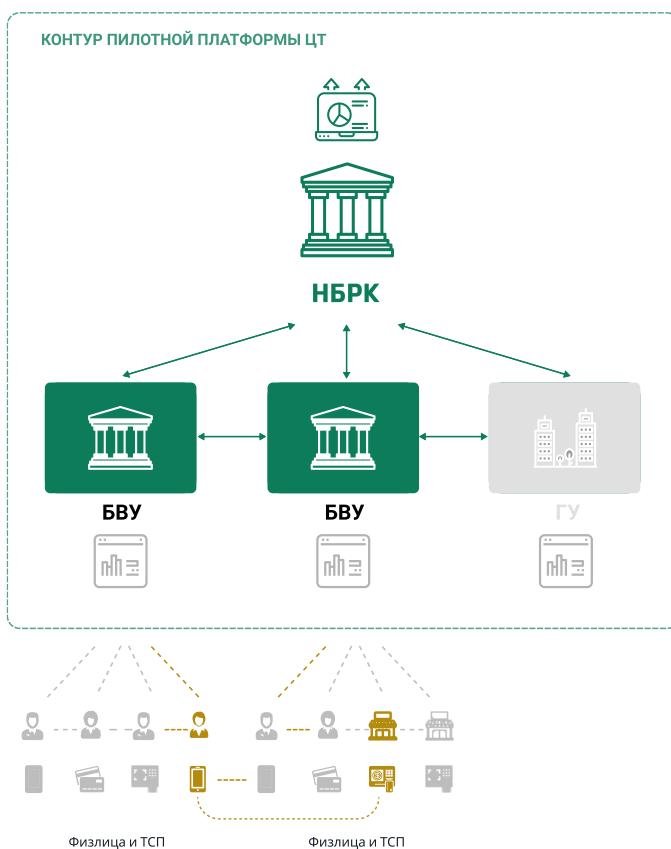
### 2.8 Покупка в режиме оффлайн

Покупка в режиме оффлайн – это перевод токенов между цифровыми кошельками на устройствах физического лица и ТСП при отсутствии интернет-соединения у обоих участников. При этом во время проведения транзакции устройства пользователей должны находиться в пределах радиуса действия NFC-соединения или аналогичного протокола близкой коммуникации.

#### Протестированные гипотезы

- **Оффлайн платежи.** Реализована возможность покупки с передачей ЦТ между двумя устройствами с цифровыми кошельками при отсутствии доступа в интернет у обоих участников расчетов (в рамках текущего PoC протестирована однократная покупка /оффлайн-транзакция без повторного использования токенов в оффлайн режиме).
- **Удобство транзакций.** Реализованный сценарий повторяет текущий опыт оплаты покупок в безналичных платежах, позволяя обеспечить как минимум тот же уровень удобства для пользователя. При этом появляется возможность цифровых операций при отсутствии интернета – доступных ранее только для наличных платежей.
- **Безопасность транзакций.** Токены позволяют однозначно установить эмитента средств даже в оффлайне. При этом для внедрения необходимо обеспечить механизмы для снижения рисков двойной траты
- **Снижение издержек обращения.** Функционал оффлайн-платежей позволит снизить долю наличного оборота и как следствие снизить издержки и риски, связанные с наличными операциями.
- **Социальные платежи.** Функционал оффлайн-платежей также реализована возможность оплаты с проверкой специального назначения токенов. Подход к ограничениям трат по специальным токенам также работает при отсутствии интернета.

### Участники сценария «Покупка в режиме оффлайн»



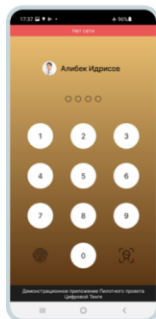
### Сценарий глазами пользователя

Одно из важнейших свойств наличных – возможность совершения операций с ними при отсутствии интернет-соединения у отправителя и получателя. Необходимость интернет-соединения является одним из ограничений электронных платежей. Так как в платформе ЦТ используется token-based модель, теоретически с ЦТ возможно проводить операции при отсутствии интернета у отправителя и получателя.

Чтобы практически протестировать данное предположение, в пилотном проекте была реализована следующая конфигурация сценария «Покупка в режиме оффлайн». ТСП может принять средства от покупателя в оффлайне, но для их дальнейшего использования требуется синхронизация этих средств в онлайн. В связи с техническими особенностями UTXO модели (см. сценарий «Онлайн-перевод») данное ограничение также накладывается на средства покупателя, полученные в качестве сдачи. Несмотря на это, реализация сценария пилотного проекта возможна для использования в случае кратковременного отсутствия интернет-соединения у пользователей.

В дальнейшем планируется проанализировать более сложные сценарии платежей в режиме оффлайн, включая проведение нескольких последовательных оффлайн-операций и введение ограничений для снижения сопутствующих рисков.

### Функциональное описание сценария «Покупка в режиме оффлайн»



#### ШАГ 0

Алибек делает заказ в кафе и сообщает, что будет оплачивать ЦТ. У Алибека отсутствует интернет-соединение



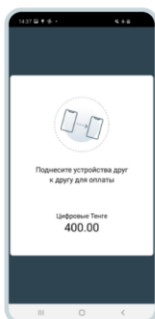
#### ШАГ 1

Кассир вводит заказ: выбирает товар из меню



#### ШАГ 2

Кассир добавляет заказ в чек. Переходит в меню «Оплата» и выбирает способ оплаты: ЦТ



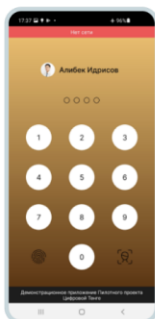
#### ШАГ 3

Кассир просит Алибека поднести устройство для оплаты. Касса находится вне сети



#### ШАГ 4

Алибек входит в приложение Банка А, нажимает «Покупка», выбирает соцкошелек



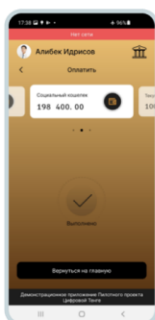
#### ШАГ 5

Алибек подтверждает разрешение на оплату через идентификацию



#### ШАГ 6

Алибек подносит телефон к устройству кассира



#### ШАГ 7

Алибек видит подтверждение оплаты и обновленный баланс соцкошелька



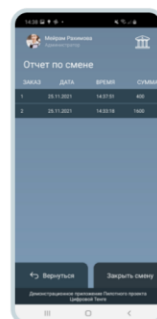
#### ШАГ 8

На устройстве кассира появляется информация об успешной продаже



#### ШАГ 9

Кассир переходит в раздел отчетов, где отражена транзакция продажи, которая ожидает синхронизации



#### ШАГ 10

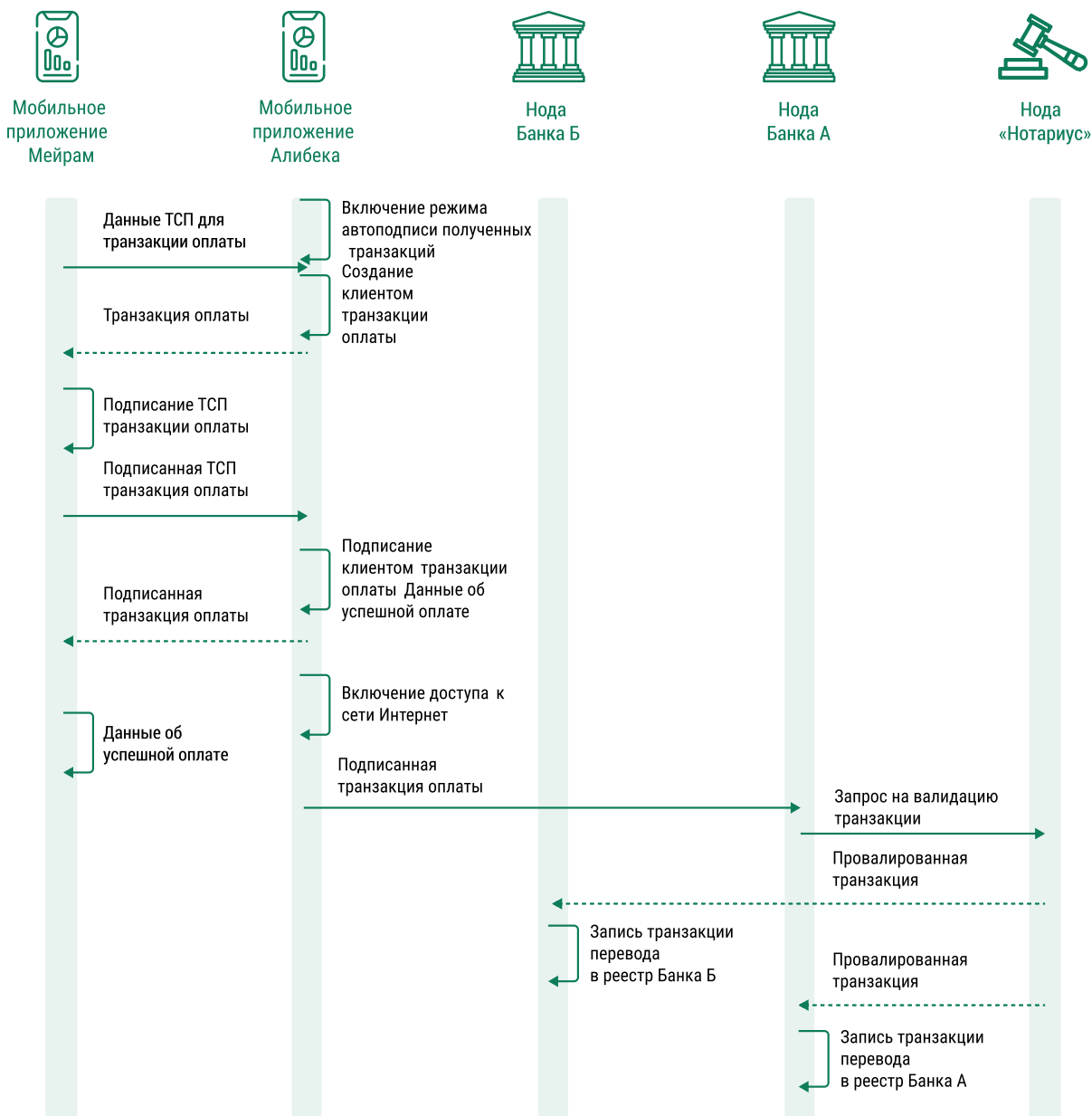
Устройство кассира подключается к интернету: транзакция синхронизируется



### Взгляд изнутри

Схема «Покупка в режиме офлайн» не сильно отличается от покупки в режиме онлайн. Однако для финализации платежа после завершения транзакции между продавцом и покупателем требуется подключение к сети хотя бы одного из них. В этот момент выполняется синхронизация: производится проверка токенов и запись транзакции в реестр.

### Взаимодействие внутри платформы – «Покупка в режиме офлайн»



### Риски и сложности для платежей в режиме оффлайн

Token-based модель позволяет реализовать надежные механизмы по ограничению рисков для участников до синхронизации токенов:

- ✓ Информация об эмитенте криптографически заложена в структуру токена, не может быть изменена и передается вместе с ним. Это исключает возможность подделки средств.
- ✓ Каждый токен уникален и хранит историю обо всех совершенных с ним транзакциях. То есть после синхронизации токенов хотя бы одним из участников платежа, с помощью данных KYC возможно точно установить личности участников подозрительных операций.

### Технические ограничения решения

Чтобы исключить возможности многократного использования токенов ЦТ, предусмотрен механизм консенсуса. Этот алгоритм реализуется с помощью нотариальной ноды и смарт-контрактов, которые определяют, какие операции можно совершать с токенами. Скрипты смарт-контрактов могут автоматически проверять выполнение базовых ограничений на операции с ЦТ, например:

1. Транзакцию с ЦТ из токена одобрил владелец токена. Для этого транзакция должна быть подписана владельцем токена.
2. Владелец токена с ЦТ – организация или физическое лицо, прошедшие процедуры KYC в БВУ. Для этого транзакция должна быть подписана БВУ, обслуживающим клиента.
3. В ходе транзакции суммарное количество ЦТ у участников транзакции не изменилось. Для этого нотариальная нода проверяет контрольные суммы входов и выходов из транзакции.

В онлайн-режиме при попытке передачи токена ЦТ, который уже был использован, нотариальная нода блокирует транзакцию.

Однако в оффлайн-сценариях, когда внешние участники недоступны, остается проблема многократной траты ЦТ. В этой связи для защиты интересов получателя должны быть обеспечены административные меры воздействия на владельцев, выполняющих мошеннические действия с ЦТ.

### 2.9 Сценарии внешних участников

В пилотном проекте были также реализованы сценарии с внешними участниками. При их реализации тестировалась возможность подключения и взаимодействия существующих игроков финансового рынка с пилотной платформой ЦТ.

По результатам открытого приглашения БВУ к участию в пилотном проекте, несколько игроков продемонстрировали готовность в сжатые сроки присоединиться к проекту и реализовать собственные сценарии с использованием ЦТ, выстроив интеграцию с пилотной платформой посредством API в тестовой среде. Сценарии к реализации были предложены непосредственно внешними участниками для проверки наиболее важных для БВУ преимуществ ЦТ.

В ходе разработки сценариев, в первую очередь, была протестирована техническая возможность подключения внешних участников к пилотной платформе, что послужило подтверждением гипотезы.

**Простой доступ.** Механизм подключения внешних участников является несложным и быстрым. Результаты тестирования показали, что сроки, ресурсы и затраты на подключение внешних участников к платформе являются адекватными.

### Подход к отбору внешних участников

В июне-июле 2021 года НБРК провел ряд открытых профильных встреч с участниками рынка, где пригласил банки и финтех-компании к участию в пилотном проекте. Основными требованиями являлись:

- ✓ опытная команда с технологической экспертизой (DLT-приложения, Dapps/Open API /IoT, SDK, REST, GraphQL, JWT, мобильная/веб-разработка)
- ✓ наличие управленческих и продуктовых компетенций, подтвержденных реализованными продуктами
- ✓ готовность оперативно мобилизовать команду для дизайна и разработки, ее доступность для ежедневной коммуникации и возможность работать в рамках гибкой методологии
- ✓ наличие собственной ИТ-инфраструктуры, приложений и специалистов для реализации проекта.

Отбор кандидатов проводился в несколько этапов:

1. На первом этапе был произведен отбор среди участников, подавших заявку и соответствующих указанным выше критериям.
2. Далее проводилась оценка сценариев, предложенных банками для реализации в рамках пилотного проекта. Сценарии должны были демонстрировать функционал платформы ЦТ.
3. На заключительном этапе проводилась оценка сроков, трудозатрат и API, требуемых для реализации сценария.

По итогам отбора к проекту присоединились и успешно реализовали собственные сценарии два БВУ: АО «Kaspi Bank» (с подключением команды «Kaspi Pay») и АО «Евразийский банк» (Eurasian Bank).

В рамках проекта совместно с внешними участниками (БВУ) были реализованы два сценария:

- ✓ **Сценарий «Погашение кредита с помощью ЦТ».** Возможность и удобство интеграции с существующими банковскими продуктами – важные факторы при проработке вопроса внедрения цифровой валюты в РК. Реализация сценария позволяет расширить спектр применения ЦТ и протестировать функциональность, важную как для клиентов банка, так и для самих БВУ. Для этого сценария рабочей группой на стороне БВУ была доработана тестовая версия мобильного приложения клиента банка. В мобильном приложении были реализованы дополнительные интерфейсы для работы с ЦТ и интеграция с пилотной платформой.
- ✓ **Сценарий «Онлайн-перевод на платформе ЦТ».** В настоящее время онлайн-перевод – одна из наиболее часто используемых клиентами банковских операций. Поэтому важно, чтобы этот сценарий был простым и интуитивно понятным пользователям – будущим владельцам ЦТ. В ходе пилотного проекта была реализована возможность онлайн-перевода между клиентами БВУ для проверки этой возможности. Для этого сценария на стороне БВУ была выполнена интеграция с платформой ЦТ.

Дополнительно был разработан и протестирован сценарий, реализованный внутренней командой пилотного проекта, включающий интеграцию с внешними приложениями:

- ✓ **Сценарий «Использование специальных токенов для оплаты медицинских услуг».** Цель реализации сценария – проверка возможности использования ЦТ со специальным назначением при оплате услуг. Использование токенов специального назначения позволяет повысить прозрачность платежей при оплате товаров и сервисов, в том числе при использовании средств государственного финансирования. В рамках сценария была реализована интеграция платформы ЦТ со специально разработанными тестовыми приложениями медицинской организации и социального фонда.

### Технологические аспекты подключения внешних участников

Внешние участники могут подключаться к ПО пилотного проекта после прохождения процедуры регистрации участника в распределенном реестре.

НБРК определяет порядок регистрации участников в платформе и контролирует их действия в распределенном реестре. Также контроль действий участников в реестре осуществляется с помощью нотариальной ноды, которая валидирует и проверяет все транзакции.

В ходе пилотного проекта была рассмотрена возможность динамического подключения участников сети. Данная функциональность учтена в архитектуре пилотной платформы и может быть реализована с помощью инструментария Corda платформы.

Взаимодействие внешних участников с пилотной платформой в рамках прототипа было реализовано посредством API, предоставляющим возможность:

- ✓ открытия и регистрации кошельков клиентов БВУ
- ✓ распределения ЦТ от БВУ клиентам БВУ

## 2.4 Сценарии пилотного проекта

### ✓ выполнения транзакций:

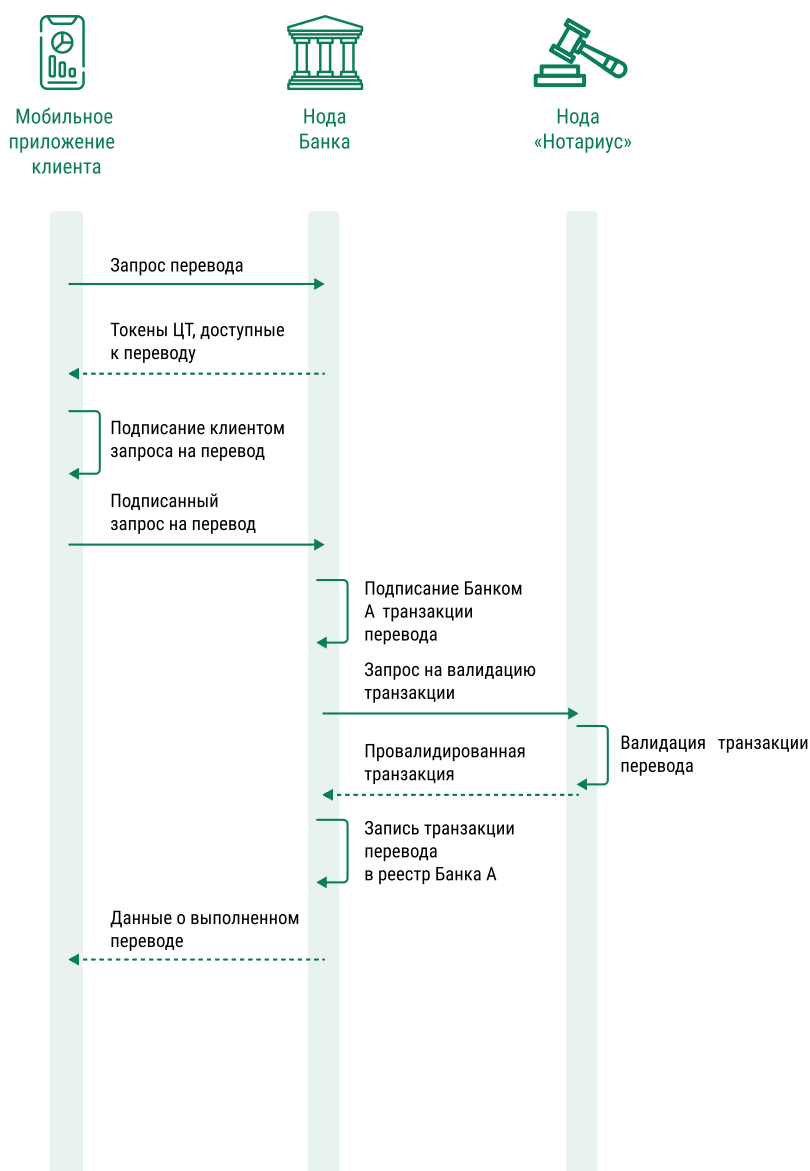
От клиентов БВУ на кошелек БВУ (от клиента участника непосредственно участнику);

От БВУ 1 к БВУ 2 (между нодами разных участников);

От клиентов БВУ к клиентам БВУ (клиентами внутри ноды одного из участников). Пример подобного взаимодействия приведен в разделе [2.4.2.6](#) далее.

Таким образом, способом взаимодействия внешних участников с платформой будет являться непосредственно Corda-платформа, обеспечивающая меры по безопасности и контролируемости выполняемых транзакций.

### Пример транзакции перевода от клиента БВУ в БВУ



Ключевые вопросы для дальнейшей проработки – технические аспекты реализации функциональности, связанной с использованием ЦТ.

### 1. Способ передачи транзакций в режиме оффлайн

Сценарий оффлайн-покупки требует двустороннего обмена между устройствами (см. раздел [2.4.2.8](#)). Поэтому в качестве возможных способов двустороннего обмена мы рассматривали только те, которые позволяют его обеспечивать. Ранее (см. раздел [2.4.2.7](#)) мы уточнили, что в качестве технологии обмена в пилотном проекте использовался протокол NFC на устройствах с ОС Android. Два этих фактора – исходные ограничения пилотного проекта. При дальнейшем более детальном изучении вопроса оффлайн-транзакций, необходимо провести исследование возможности использования реализованных алгоритмов для оффлайн-транзакций для устройств с другими ОС (в частности, iOS). Также при дальнейшей проработке задачи оффлайн-транзакций необходимо провести анализ возможных ограничений реализованных алгоритмов при масштабировании решения.

### 2. Выполнение процедур KYC для БВУ

БВУ хранят информацию о своих клиентах, подписывают их транзакции и могут идентифицировать своего клиента в транзакции с помощью операционного ключа кошелька клиента.

Поэтому с течением времени у БВУ сохраняются данные обо всех использованиях токенов ЦТ, которые когда-либо были у БВУ или его клиентов. Это требует выделения дополнительных мощностей в инфраструктурах БВУ, участников распределенного реестра.

В ходе пилотного проекта не проводился анализ и расчет объемов информации, которые могут быть сгенерированы за определенный период. Этот вопрос требует дополнительной проработки, в том числе со стороны БВУ, так как объем хранимых данных также напрямую зависит от дополнительных параметров транзакций и данных клиентов, которые могут быть заданы участниками как обязательные к передаче для осуществления процедур идентификации клиентов.

### 3. Реализация цепочек оффлайн-транзакций

Когда пользователь производит перевод или оплату в режиме онлайн, после проверки транзакции нотариальной нодой транзакция записывается в реестры участников, которые участвовали в транзакции. Например, клиент Банка А произвел оплату с мобильного устройства в режиме онлайн в ТСП, которое обслуживается в Банке Б. Транзакция оплаты в режиме онлайн будет сохранена в реестрах банков А и Б. Поэтому если после этого клиент банка Б сделает перевод клиенту Банка А, история транзакций клиента Банка А будет последовательной и корректной.

В случае, если клиент Банка А производит оплату в ТСП, которое обслуживается в Банке Б, с помощью устройства, находящегося вне зоны доступа сети Интернет, синхронизация и запись транзакций в реестры банков А и Б произойдет только после того, как устройство получит доступ в сеть Интернет. Например, может произойти следующая ситуация:

1. 10.11 10:00 Клиент Банка А оплачивает покупку в ТСП банка Б в режиме оффлайн;
2. 10.11 11:00 Клиент Банка Б переводит клиенту банка А некоторое количество ЦТ в режиме оффлайн;
3. 10.11 11:30 Клиент Банка А оплачивает еще одну покупку в ТСП банка Б в режиме оффлайн.

При этом на мобильном устройстве клиента Банка А будет сохранена цепочка оффлайн транзакций, которая будет добавлена в историю транзакций по кошельку клиента после того, как его мобильное устройство получит доступ к сети Интернет.

Транзакции по кошельку клиента должны быть собраны в цепочку и связаны между собой в виде ссылок друг на друга. Когда транзакции выполняются клиентом в оффлайне, при включении сети «Интернет» информацию о выполненных операциях необходимо встроить в циклический граф транзакций клиента, который построен по данным о транзакциях между его кошельком и нодами других участников. Чем больше оффлайн-транзакций выполнит клиент, тем сложнее будет процесс валидации и синхронизации транзакций.

Для соблюдения требований ПОД/ФТ БВУ клиента в режиме онлайн подписывают транзакции клиентов. Когда клиент получает токены в режиме оффлайн, банк не участвует в процессе подписи и проверки требований ПОД/ФТ. Поэтому клиент не сможет использовать токены ЦТ, полученные в режиме оффлайн. Чтобы он мог использовать токены, полученные из оффлайн-транзакции, у него должна быть возможность проводить транзакцию без участия БВУ, которая может быть записана в распределенный реестр после синхронизации. Возможность и способ реализации такой функциональности также требует дальнейшей проработки на следующих этапах.

#### 4. Использование легких клиентов платформы

Теоретически клиенты могут проводить транзакции без подписи со стороны БВУ. Для этого можно использовать легкие клиенты ядра платформы. На момент разработки ПО пилотного проекта в Corda не была реализована библиотека для подписи транзакций клиентом без участия банка. Поэтому сценарий использования токенов ЦТ, полученных клиентом в оффлайн-режиме до момента синхронизации данных с распределенным реестром не был проверен в ходе пилотного проекта.



В случае, если ядро пилотной платформы будет предоставлять возможность полной подписи транзакций клиентом в оффлайн-режиме, клиент сможет использовать токены ЦТ после их получения в оффлайне до момента синхронизации. При этом необходимость синхронизации как таковой все еще остается для соблюдения требований ПОД/ФТ и решения проблем двойных трат полученных токенов ЦТ.

Вопрос использования легких клиентов в платформе требует дополнительной проработки как с технологической стороны, после реализации возможности подписи на стороне Corda r3, так и с административной, для выработки мер ПОД/ФТ и для противодействия мошенничеству.

### 5. Возможности масштабирования

Возможность масштабирования пилотной платформы – важный аспект для учета при проектировании и разработке платформы ЦТ. Возможные направления анализа масштабируемости решения это: 1) архитектура нод участников (включая возможность репликации и параллелизации частей реестра и балансировки нагрузки); 2) использование off-chain транзакций для сокращения нагрузки на DLT [\[10\]](#).

При этом дальнейший анализ масштабируемости и расширяемости решения должен проводиться с учетом выбранного ядра платформы. Ранее проводились исследования возможностей масштабирования r3 Corda, например, совместное исследование возможности реализации пост-трейдинговой обработки акций США на базе распределенного реестра. Результаты, представленные DTCC, Accenture, Digital Asset и r3, показали, что Corda способна поддерживать более 100 млн сделок в день [\[11\]](#). Также проводился анализ «пропускной способности» (максимального количества запросов за период времени) реестра с 4 Corda-нодами, которые показали, что в такой конфигурации Corda способна поддерживать 300 запросов в секунду [\[12, 13\]](#).

Для оценки возможности масштабирования платформы ЦТ необходимо проведение экспериментов с учетом особенностей целевой архитектуры, включая:

- характер взаимодействия участников в ходе различных сценариев (многоэтапность и последовательность взаимодействия)
- структуру транзакций разных типов
- количество и архитектуру нод-участников распределенного реестра
- особенности инфраструктуры платформы
- прогнозное количество пользователей ЦТ.

### 6. Открытые вопросы

С учетом вышеупомянутых ключевых вопросов для проработки на следующих этапах можно отметить следующие развилки для внедрения ЦТ, по которым еще предстоит найти решения:

#### Ключевые развилки и аспекты для дальнейшей проработки

Наименование	Краткое описание	Решение для пилота и аспекты дальнейшей проработки
<b>Централизованные vs децентрализованные кошельки</b>	<p>Варианты:</p> <ol style="list-style-type: none"> <li>1) Разные кошельки в разных банках в соответствии с двухуровневой моделью</li> <li>2) НБРК управляет единым кошельком, а БВУ только открывают кошельки</li> </ol>	<p>В пилотном проекте предусмотрена двухуровневая модель: БВУ открывают и обслуживают кошельки клиентов, НБРК осуществляет эмиссию и устанавливает участников.</p> <p>При использовании данной модели в перспективе может оказаться актуальной реализация возможности по управлению кошельками клиента из «единого окна» (через механизмы доступа к данным и инициации транзакций в БВУ посредством Open API) и гибкость в реализации под-кошельков.</p>
<b>Анонимность / конфиденциальность vs прозрачность и ПОД/ФТ</b>	<p>Сохранение свойств наличных платежей предполагает возможность анонимности / непрозрачности транзакций для других. При этом в соответствии с требованиями к ПОД/ФТ, БВУ должны иметь возможность идентифицировать, отслеживать и хранить транзакции их клиентов</p>	<p>Предложено решение «настраиваемой анонимности»: только БВУ, обслуживающие клиентов, имеют доступ к транзакциям своих клиентов. При этом внешним участникам информация об участниках платежа не доступна. Пользователи могут сами выбрать показывать ли персональные данные другим пользователям, участвующим в транзакции.</p> <p>Вопрос отслеживаемости транзакций распределенного реестра НБРК, а также регулирования этого процесса требует дополнительной проработки как с регуляторной, так и с технологической стороны.</p>
<b>NFC vs другие технологии оффлайна</b>	<p>Осуществление двустороннего обмена между двумя устройствами возможно с использованием разных технологий, в том числе:</p> <ul style="list-style-type: none"> <li>•NFC</li> <li>•Wi-Fi direct</li> <li>•Bluetooth</li> <li>•и другие методы обмена</li> </ul>	<p>В пилотном проекте реализовано использование NFC при оффлайн-покупке. При дальнейшей реализации могут быть дополнительно исследованы альтернативные решения (как с точки зрения потребительского опыта, так и технологической реализуемости), что позволит принять решение, какая технология обмена данными будет использована.</p>

## 2.5 Технологические аспекты для дальнейшей проработки

Наименование	Краткое описание	Решение для пилота и аспекты дальнейшей проработки
<b>Время в оффлайне vs риск двойной траты</b>	Пользователи могут совершать покупки при отсутствии интернета как у клиента, так и у продавца, но при этом возникают риски двойной траты (риски того, что при сложной технологической атаке может быть проведена транзакция с токенами, которые уже были потрачены)	В пилотном проекте был реализован и протестирован функционал платежей в режиме оффлайн, детальной проработки механизмов митигации рисков двойной траты не проводилось. Для внедрения промышленного решения необходимо провести работу по оценке и снижению рисков двойной траты (через комбинацию операционных, регуляторных и технологических мер).
<b>История токена vs производительность</b>	Токен хранит историю о транзакциях. Чем больше транзакций проведено с токеном, тем больше данных нужно передать при каждой последующей транзакции.	На следующих этапах проекта должно быть проведено тестирование производительности и выработано решение по перевыпуску токена для очистки его истории.
<b>Конфиденциальность vs возможность восстановления кошельков</b>	Конфиденциальность токенов – это важное свойство платежной системы. При этом абсолютная конфиденциальность не позволяет восстановить кошелек в случае утери доступа к нему.	Предполагается, что выбранная механика по управлению ключами пользователей в пилотном проекте позволит восстанавливать кошельки пользователей без влияния на конфиденциальность транзакций.  Необходима отдельная проработка процедуры и технологии восстановления кошельков в рамках следующих этапов.
<b>Анонимность vs программируемость</b>	Для проверки валидности токенов в транзакции получатель должен иметь возможность выполнить смарт-контракты для всех транзакций, которые были отражены в истории токена. Поэтому смарт-контракты не могут оперировать суммами транзакций, балансов и персональными данными участников и клиентов, так как эти данные скрыты для получателей.	Необходимо найти баланс между анонимностью и программируемостью:  некоторые контракты могут использовать специальные криптографические средства (например, варианты non-interactive ZKP), чтобы реализовать ограничения без разглашения частных данных, однако для участия в других контрактах, возможно, придется пожертвовать приватностью, разгласив часть данных о токенах.  Целевое решение должно быть выбрано по результатам технологического исследования возможностей создания смарт-контрактов на платформе ЦТ.

## 2.6 Сравнение с проектами ЦВЦБ в других странах

Статистика BIS на октябрь 2021 года по обзору инициатив ЦВЦБ по всему миру приводит данные о 26 странах, где центральные банки уже реализуют пилотные проекты. На разных рынках с учетом их локальной специфики и потребностей рынка, центральные банки выбирают свои подходы и варианты реализации CBDC, комбинируя новые технологии, опробованные на альтернативных валютах, с традиционными.

Наиболее релевантным является опыт стран, существенно продвинувшихся в создании токенизированных розничных цифровых валют с уже выстроенным взаимодействием центрального банка и других игроков финансового рынка.

### Сравнение проектов ЦВЦБ в других странах

СТРАНА	ГОД	ЦЕЛИ	ТЕКУЩИЙ СТАТУС	КЛЮЧЕВЫЕ ОСОБЕННОСТИ
 КИТАЙ	2014	<ul style="list-style-type: none"> <li>Обеспечение финансовой доступности и развитие конкуренции</li> <li>Повышение эффективности трансграничных расчетов</li> </ul>	<ul style="list-style-type: none"> <li><b>Опытная эксплуатация</b> (тестирование – 9 городов, 140 млн пользователей)</li> <li><b>Кросс-граничное</b> тестирование планируется на Олимпиаде – 2022 года</li> </ul>	<ul style="list-style-type: none"> <li><b>Гибридная</b> (на основе счета и токенов)</li> <li><b>Один кошелек в одном банке</b> (+ суб-кошельки)</li> <li><b>Анонимные транзакции</b> (на небольшой объем)</li> <li>Оффлайн (LCD-карты)</li> </ul>
 ШВЕЦИЯ	2017	<ul style="list-style-type: none"> <li>Снижение уровня использования наличных денег в стране</li> <li>Повышение доступности денег центрального банка</li> </ul>	<ul style="list-style-type: none"> <li>Реализована 1-я фаза пилота с 2020-2021 гг.</li> <li>Прорабатывается <b>регулирование и технологические аспекты</b></li> </ul>	<ul style="list-style-type: none"> <li><b>Децентрализованная</b> (на основе токенов, DLT)</li> <li><b>Несколько кошельков</b> в нескольких банках</li> <li>Контролируемый уровень <b>анонимности</b></li> <li><b>Долгосрочный оффлайн</b></li> </ul>
 РОССИЯ	2020	<ul style="list-style-type: none"> <li>Повышение <b>скорости, удобства</b> и безопасности платежей</li> <li>Снижение объема <b>наличных</b></li> </ul>	<ul style="list-style-type: none"> <li>Реализация <b>прототипа</b> платформы до <b>конца 2021</b></li> <li>Запланировано <b>пилотирование на 2022</b> с 12 банками</li> </ul>	<ul style="list-style-type: none"> <li><b>Гибридная</b> (онлайн-счет, оффлайн-токен)</li> <li><b>Один кошелек. Доступ из нескольких банков</b></li> <li>Отсутствие <b>анонимности</b></li> <li><b>Оффлайн</b> (в проработке)</li> </ul>
 ЕС	2020	<ul style="list-style-type: none"> <li>Поддержка <b>цифровизации</b> и стратегической <b>независимости ЕС</b></li> <li>Увеличение <b>роли евро</b> в международной торговле</li> </ul>	<ul style="list-style-type: none"> <li><b>Принято решение</b> о старте пилота</li> </ul>	<ul style="list-style-type: none"> <li><b>В проработке</b></li> </ul>
 США		<ul style="list-style-type: none"> <li>Поддержку доллара как международной <b>резервной валюты</b></li> <li>Снижение <b>уровня</b> использования <b>наличных</b></li> </ul>	<ul style="list-style-type: none"> <li><b>Digital Dollar Foundation</b> – запланировано 5 <b>пилотных программ</b> до середины 2022</li> </ul>	<ul style="list-style-type: none"> <li><b>Децентрализованная</b> (на основе токенов, DLT)</li> <li><b>Оффлайн</b> (в проработке)</li> </ul>

## 2.6 Сравнение с проектами ЦВЦБ в других странах

Среди этих стран наибольшего прогресса из актуальных для Казахстана юрисдикций достигли проекты следующих центральных банков:

- **Национальный банк Китая** больше всего продвинулся во внедрении ЦВЦБ – параллельно с планомерным развертыванием e-CNY на локальном рынке, PBOC уже реализует пилотные проекты с соседними странами по кросс-граничному использованию ЦВЦБ.
- **Банк Швеции**, который раньше всех в Европе приступил к пилотированию, сейчас прорабатывает регуляторный подход к внедрению, параллельно с детальной поэтапной проработкой технологических аспектов совместно с банками и вендорами устройств.
- **Банк России** определился с концепцией и включился в разработку технологической платформы, анонсировав пилотирование с 12 банками в 2022 году.

Среди ключевых особенностей внедрения ЦВЦБ в этих странах в сравнении с НБРК можно выделить следующие:

- ✓ Во всех вышеуказанных странах, как и в Казахстане, изучается **двухуровневая модель** цифровой валюты, при которой центральный банк разрабатывает дизайн и базовый функционал платформы, а БВУ и прочие финансовые организации несут ответственность за подключение граждан и предоставление сервисов населению.
- ✓ **Тип доступа** влияет на построение транзакций внутри платформы, возможности программирования, конфигурации приватности участников транзакций. В то время как Швеция аналогично выбору НБРК использует модель учета на основе токена, банки Китая и России основывают дизайн своих валют на гибридной модели: промежуточная модель как с элементами модели на основе токенов, так и традиционной модели счетов.
- ✓ **Хранение токенов пользователя** влияет на возможность оффлайн-платежей. Банк Швеции в рамках пилотирования e-кроны выбрал подход с хранением токенов пользователей на нодах их банков. В Казахстане реализована модель хранения токенов на устройстве пользователя, что обеспечивает возможность платежей в режиме оффлайн при внезапном отключении Интернета.
- ✓ Все центральные банки высказали заинтересованность во внедрении функционала для проведения платежей в **режиме оффлайн**. В настоящее время в Казахстане реализован функционал оффлайн-платежей на пилотной платформе: пользователи могут совершать покупки при отсутствии интернета как у клиента, так и продавца. Из открытых источников известно, что Китай и Швеция приступили к тестированию технологической реализации данного вида транзакций. Информация о стадии проработки данного вопроса в других странах отсутствует.
- ✓ В Китае реализован подход «контролируемой анонимности» с разными уровнями раскрытия информации о транзакции, в том числе с зависимостью от суммы перевода. Банк Швеции также рассматривает возможность реализации разных уровней анонимности для кошельков пользователей. Банк Казахстана в рамках пилотного проекта протестировал концепцию настраиваемой анонимности с возможностью управления доступом к информации о транзакциях и опцией настройки сокрытия данных по желанию пользователя: пользователи могут сами выбирать, показывать ли персональные данные другим участникам транзакции.


## 2.6 Сравнение с проектами ЦВЦБ в других странах

- ✓ **Программируемость.** В рамках пилотного проекта в Казахстане реализована программируемость, которая позволяет закладывать ограничения на траты в структуру самого токена (целевое использование). Публичная информация о возможности настраивания целевого использования токенов в других странах отсутствует.

В результате анализа развития проектов по разработке ЦВЦБ в мире можно сделать вывод, что большинство центральных банков уже включилось в гонку, но зрелой и устоявшейся практики пока нет – это все еще зона для исследований и экспериментов. Сейчас можно утверждать, что несмотря на принятую единую архитектурную модель цифровых валют в указанных выше странах, прочие параметры будут варьироваться в зависимости от преследуемых целей и выбранных решений по базовым развилкам.

По результатам пилотного проекта был определен перечень открытых вопросов, которые необходимо будет рассмотреть в дальнейшем для возможности внедрения ЦТ.





Экономические и  
регуляторные аспекты

стр. **71-88**



Из-за отсутствия международного опыта в решении вопросов полноценного внедрения ЦВЦБ в систему финансово-экономических отношений остается открытым вопрос о последствиях и рисках экономического характера, которые могут возникнуть в результате эмиссии ЦВЦБ.

Выделяют три ключевых направления, в рамках которых подобные риски могут возникать и реализовываться:

1. влияние эмиссии ЦВЦБ на объем денежного предложения, инфляционные процессы и, соответственно, устойчивость денежно-кредитной политики страны, а также трансмиссионные каналы
2. реакция финансового сектора на внедрение ЦВЦБ в контексте финансовой стабильности
3. воздействие ЦВЦБ на актуальные и перспективные бизнес-условия финансового сектора.

В рамках пилотного проекта для того, чтобы протестировать указанные риски в текущих условиях казахстанской экономики, была сформулирована и проработана теоретическая экономическая модель ЦТ. Важно отметить, что подобная модель в настоящее время не является конечным и исчерпывающим методологическим подходом в рамках экономического анализа ЦТ. Следовательно, в дальнейшем по мере сбора эмпирических данных и количественной оценки теоретических параметров модель может дополняться, видоизменяться и расширяться. Вместе с тем уже на данном этапе модель позволяет при первом приближении проанализировать ряд экономических аспектов эмиссии и внедрения ЦТ.

### **Теоретическая экономическая модель ЦТ**

Теоретическая экономическая модель ЦТ основывается на выбранном в рамках пилотного проекта техническом дизайне эмиссии цифровой валюты, где предполагается двухуровневая цифровая платежная система с участием трех агентов в лице НБРК, банков второго уровня (БВУ) и конечного клиента.

В рамках данного дизайна эмиссия ЦТ происходит по запросу БВУ в НБРК, после – НБРК начисляет на цифровой кошелек БВУ запрошенный объем ЦТ и списывает аналогичную сумму средств с корреспондентского счета БВУ (см. рисунок ниже). Далее БВУ по запросу клиента начисляет на его цифровой кошелек необходимую сумму ЦТ, взамен списывая с текущего счета соответствующий объем безналичных средств.

### Технический дизайн эмиссии ЦТ



С учетом технического дизайна эмиссии ЦТ его теоретическая экономическая модель предполагает наличие трех экономических агентов:

- НБРК – единственный и конечный эмитент ЦТ
- Банк А – банк второго уровня, оказывающий клиентам финансовые услуги
- Алибек – физическое лицо, клиент Банка А

В рамках теоретической модели рассматривается влияние эмиссии и перетока ЦТ между агентами на основе анализа их упрощенных балансов. При этом применение упрощенных балансов экономических агентов позволяет анализировать динамику ЦТ в разрезе условных показателей денежно-кредитной статистики, а именно:

- $RM$  – денежная база (или резервные деньги), которая включает в себя прямые обязательства НБРК в виде наличных средств вне банка, его корреспондентские счета и средства на счете цифрового кошелька (так называемые «цифровые наличные средства»)
- $M0$  – денежный агрегат, через который учитываются наличные средства в обращении
- $M0_{dt}$  – денежный агрегат, отражающий объем эмитированного НБРК ЦТ («цифровые наличные средства»)
- $C$  – текущие (безналичные) счета клиентов в Банке А
- $M1$  – условный денежный агрегат, представляющий широкое денежное предложение, как сумма компонент  $M0$ ,  $M0_{dt}$  и  $C$ .

### 3.1 Экономические аспекты внедрения ЦТ

В рамках теоретической модели в формате балансов экономических агентов были изучены три стадии эмиссии ЦТ с учетом его влияния на показатели денежно-кредитной статистики:

- Первая стадия: ситуация в экономике до эмиссии ЦТ.
- Вторая стадия: эмиссия ЦТ в виде его начисления НБРК на цифровой кошелек банка А.
- Третья стадия (вариант 1): начисление ЦТ с цифрового кошелька банка А на цифровой кошелек Алибека – клиента банка А на основе конвертации безналичных средств с текущего счета.
- Третья стадия (вариант 2): начисление ЦТ на цифровой кошелек Алибека – клиента Банка А на основе конвертации наличных денег.

Далее рассмотрим теоретическую модель эмиссии ЦТ поэтапно, следуя отмеченным выше стадиям.

#### Первая стадия. В экономике отсутствует ЦТ

##### Балансы экономических агентов до эмиссии ЦТ (тенге в текущих ценах)

НБРК			
Активы		Пассивы	
Вне рассмотрения		Корр. счет Банка А	3000
		Наличные деньги вне НБРК	1550
		Цифровой кошелек ЦТ (резервы ЦТ)	0

Банк А			
Активы		Пассивы	
Корр. счет Банка А в НБРК	3000	Текущий счет Алибека	700
Наличные деньги Банка А	1000	Другие клиенты	3300
Цифровой кошелек ЦТ Банка А	0		

Алибек			
Активы		Пассивы	
Текущий счет в Банке А (С)	700	Вне рассмотрения	
Наличные деньги (М0)	550		
Цифровой кошелек Алибека	0		

### 3.1 Экономические аспекты внедрения ЦТ

В рамках первой стадии, которая отражает исходную ситуацию в экономике, когда НБРК не производил эмиссии ЦТ, условно предполагаются следующие размеры денежных средств в экономике:

- 3000 тенге в виде корреспондентского счета банка А (часть денежной базы RM)
- 1000 тенге – наличные деньги вне НБРК (часть денежной базы RM)
- 700 тенге – объем текущего счета Алибека (часть компонента С, включаемая в широкое денежное предложение M1)
- 3300 тенге – объем текущего счета других клиентов банка А (вне аналитического рассмотрения динамики ЦТ, является частью компонента С)
- 550 тенге – наличные деньги Алибека (денежный агрегат M0).

Таким образом, можно посчитать, что в разрезе денежно-кредитной статистики исходная ситуация в экономике выглядит следующим образом:

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

### 3.1 Экономические аспекты внедрения ЦТ

#### Вторая стадия . НБРК по запросу банка А эмитирует

#### Балансы экономических агентов после эмиссии ЦТ (тенге в текущих ценах)

НБРК			
Активы		Пассивы	
Вне рассмотрения		Корр. счет Банка А	2000
		Наличные деньги вне НБРК	1550
		Цифровой кошелек ЦТ (резервы ЦТ)	1000
Банк А			
Активы		Пассивы	
Корр. счет Банка А в НБРК	2000	Текущий счет Алибека	700
Наличные деньги Банка А	1000	Другие клиенты	3300
Цифровой кошелек ЦТ Банка А	1000		
Алибек			
Активы		Пассивы	
Текущий счет в Банке А (С)	700	Вне рассмотрения	
Наличные деньги (М0)	550		
Цифровой кошелек Алибека	0		

На второй стадии НБРК выпускает 1000 тенге в виде ЦТ по запросу Банка А. При этом в пассивах баланса НБРК и, следовательно, в активах баланса Банка А на цифровой кошелек начисляются 1000 тенге в качестве цифрового аналога наличных средств. В то же время начисление 1000 единиц ЦТ происходит за счет списания аналогичной суммы средств с корреспондентского счета Банка А в НБРК, что отражается на балансе двух экономических агентов.

В результате данной операции можно заметить, что суммарный объем пассивов НБРК (денежная база) не изменяется, равно как и объем активов Банка А. Вместе с тем, происходит изменение структуры денежной базы и активов Банка А.

Таким образом, на второй стадии ключевые показатели денежно-кредитной статистики в виде денежной базы RM и широкого денежного предложения M1 остаются неизменными, составляя 4550 тенге соответственно.

### 3.1 Экономические аспекты внедрения ЦТ

Третья стадия (вариант 1). Начисление ЦТ на счет цифрового кошелька Алибека на основе использования текущего счета

**Балансы экономических агентов после начисления ЦТ на счет конечного клиента на основе конвертации безналичных средств (тенге в текущих ценах)**

#### НБРК

Активы		Пассивы	
Вне рассмотрения		Корр. счет Банка А	<b>2000</b>
		Наличные деньги вне НБРК	<b>1550</b>
		Цифровой кошелек ЦТ (резервы ЦТ)	<b>1000</b>

#### Банк А

Активы		Пассивы	
Корр. счет Банка А в НБРК	<b>2000</b>	Текущий счет Алибека	<b>200</b>
Наличные деньги Банка А	1000	Другие клиенты	3300
Цифровой кошелек ЦТ Банка А	<b>500</b>		

#### Алибек

Активы		Пассивы	
Текущий счет в Банке А (С)	<b>200</b>	Вне рассмотрения	
Наличные деньги (М0)	<b>550</b>		
Цифровой кошелек Алибека	<b>500</b>		

Третья стадия теоретической модели описывает момент непосредственного начисления цифрового аналога тенге на кошелек Алибека в размере 500 тенге. При этом в первом варианте данный процесс выполняется по запросу Алибека в Банк А, в рамках которого на кошелек ЦТ Алибека поступает сумма средств в размере 500 тенге, аналогичная сумма списывается с текущего счета клиента, который находится в пассивах Банка А. В итоге, в пассивах Банка А размер текущего счета, принадлежащего Алибеку, снижается на 500 тенге. На такой же объем сокращается размер средств на цифровом кошельке, который на второй стадии был начислен НБРК. Иными словами, после начисления 500 тенге в цифровом виде на кошелек Алибека в целом на данную величину снижается общий баланс Банка А.

### 3.1 Экономические аспекты внедрения ЦТ

В свою очередь, в активах Алибека происходит переток средств из текущего счета на кошелек ЦТ. Как можно заметить, в этом случае ЦТ, как и наличные деньги, остается в качестве обязательств НБРК, а не Банка А.

Если рассмотреть данную стадию эмиссии ЦТ через призму показателей денежно-кредитной статистики, то будет наблюдаться следующее:

- RM = 4550 тенге
- M0 = 550 тенге
- M0\_dt = 500 тенге
- C = 3500 тенге
- M1 = 4550 тенге

**Третья стадия (вариант 2). Начисление ЦТ на счет цифрового кошелька Алибека на основе использования наличных денег**

**Балансы экономических агентов после начисления ЦТ на счет конечного клиента на основе конвертации наличных средств (тенге в текущих ценах)**

#### НБРК

Активы		Пассивы	
Вне рассмотрения		Корр. счет Банка А	2000
		Наличные деньги вне НБРК	1550
		Цифровой кошелек ЦТ (резервы ЦТ)	1000

#### Банк А

Активы		Пассивы	
Корр. счет Банка А в НБРК	2000	Текущий счет Алибека	700
Наличные деньги Банка А	1500	Другие клиенты	3300
Цифровой кошелек ЦТ Банка А	500		

#### Алибек

Активы		Пассивы	
Текущий счет в Банке А (С)	700	Вне рассмотрения	
Наличные деньги (M0)	50		
Цифровой кошелек Алибека	500		



### 3.1 Экономические аспекты внедрения ЦТ

Другой вариант третьей стадии теоретической модели эмиссии ЦТ предполагает, что клиент Банка А – Алибек – для начисления ЦТ на свой кошелек в размере 500 тенге будет использовать наличные деньги. В этом случае наличные деньги Алибека поступят на соответствующий счет в активах Банка А, а аналогичный размер ЦТ будет перечислен с цифрового кошелька банка А на цифровой кошелек Алибека. В результате останутся прежними размеры балансов как у Банка А, так и у клиента. В денежно-кредитной статистике этот процесс отразится следующим образом:

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

Далее сравним изменения в показателях денежно-кредитной статистики в ситуациях до эмиссии ЦТ и после его поступления на счет конечного клиента Банка А: как за счет использования наличных денег, так и на основе применения средств на безналичном (текущем) счете.

**Условные показатели денежно-кредитной статистики до и после эмиссии ЦТ (тенге в текущих ценах)**

Показатели денежно-кредитной статистики	До эмиссии ЦТ	После эмиссии ЦТ: вариант, при котором конвертация ЦТ происходит за счет безналичных средств клиента	После эмиссии ЦТ: вариант, при котором конвертация ЦТ происходит за счет наличных средств клиента
Денежная база, $RM$	4550	4550	4550
Наличные деньги в обращении, $M0$	550	550	50
Цифровые наличные деньги в обращении, $M0_{dt}$	0	500	500
Текущие (безналичные) средства, $C$	4000	3500	4000
Денежное предложение, $M1$ ( $M0+M0_{dt}+C$ )	4550	4550	4550

Как можно заметить из представленной выше таблицы, эмиссия ЦТ ни в одном из двух вариантов не приводит ни к увеличению денежной базы (пассивов НБРК), ни к расширению денежного предложения.

Вместе с тем, при эмиссии ЦТ и его начислении на счет клиента на основе конвертации текущего счета происходят лишь изменения в структуре денежного предложения, а именно – снижение объема текущих счетов за счет роста объемов ЦТ. В случае, когда конвертация ЦТ произойдет при использовании наличных денег, в структуре денежного предложения не изменится размер текущих счетов, но произойдет сокращение наличных денег в обращении.

Таким образом, главный результат, полученный при анализе теоретической экономической модели ЦТ, сводится к следующему. При эмиссии цифрового аналога наличных средств не произойдет увеличения денежной базы и денежной массы в экономике Казахстана, а будут наблюдаться лишь изменения структуры в денежном предложении.

#### **Из этого вытекают следующие экономические выводы:**

1. Эмиссия ЦТ не оказывает влияния на расширение денежного предложения, поэтому прямого воздействия на совокупный спрос со стороны экономических агентов также не ожидается. Следовательно, инфляционные процессы остаются вне прямого или исключительного эффекта эмиссии ЦТ.
2. Эмиссия ЦТ не несет значимых или неконтролируемых рисков для финансового рынка как в случае конвертации наличных средств конечных клиентов, так и при предпочтении клиентами БВУ конвертировать в ЦТ часть своих текущих (безналичных) счетов. Так, в настоящее время в банковском секторе Казахстана наблюдается наличие избыточного уровня резервов, который сможет полностью покрыть возможные варианты снижения текущих счетов.
3. НБРК в рамках использования инструментов денежно-кредитной политики при необходимости, связанной с возможным чрезмерным оттоком средств на текущих счетах БВУ в счета ЦТ клиентов, потенциально сможет в полной мере обеспечить требуемый для БВУ объем ликвидности. Данный фактор позволит нивелировать риски «цифрового бегства», когда в кризисные моменты клиенты банков могут быть мотивированы максимальной конвертацией безналичных средств в ЦТ. Обозначенный фактор снижает также риски значительного отклонения ставок на денежном рынке от актуальных в моменте уровней базовой ставки.
4. Риски «цифрового бегства» могут ограничиваться механизмами лимитирования допустимых объемов конвертации текущих счетов в ЦТ и другими мерами финансового регулирования.

5. Представленные выше выводы указывают на то, что процесс эмиссии и использования ЦТ в качестве третьей формы фиатных денег 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.
6. В части воздействия ЦТ на действующие и перспективные бизнес-условия финансового сектора следует отметить следующее:
  - применение ЦТ потенциально позволяет осуществить больший охват финансовыми услугами потенциальных клиентов, ранее остававшихся «в тени наличности» из-за географических, технических, культурных и поведенческих ограничений и особенностей, в том числе в рамках дальнейшей интеграции клиентов в собственные экосистемы финансовых организаций
  - внедрение ЦТ создает инфраструктурные условия для разработки совершенно новых финтех-продуктов на основе преимуществ «цифровой наличности», более быстрых и дешевых финтех-сервисов (например, Embedded Finance, M2M payments, IoT-enabled payments и пр.)
  - при текущей платформенной (экосистемной) бизнес-модели финансовых организаций использование ЦТ конечными клиентами приведет к снижению зависимости ряда финансовых организаций от «транзакционной модели заработка», стимулируя их к работе в условиях «экономии масштаба» и наращиванию «сетевых эффектов» в рамках новых направлений финансовой деятельности.

#### **Следующие шаги по экономическим аспектам ЦТ**

В дальнейшем будет проведено исследование поведенческих аспектов потребителей финансовых услуг в Казахстане в отношении их паттернов, связанных с применением действующих платежных средств в виде наличных и безналичных денег в рамках торгово-экономических операций на внутреннем рынке, а также в части потенциального использования для тех же целей ЦТ. Предполагается, что данное исследование будет реализовано в том числе путем проведения опросов и фокус-групп, что позволит собрать и накопить критический набор эмпирических данных.

Вместе с тем планируется проведение полноценного научно-практического исследования для глубинного изучения макроэкономических эффектов применения ЦТ, которое в том числе будет базироваться на данных, полученных во время опросов потребителей финансовых услуг. Ожидается, что результаты данного исследования позволят дать количественную оценку параметрам, представленным в теоретической экономической модели ЦТ, которая была сформулирована на этапе пилотного проекта.

Немаловажными экономическими аспектами, которым также будет уделено особое внимание, являются вопросы, связанные с трансграничными платежами и импортными операциями, основанными на применении ЦТ.

Создание полноценной регуляторной среды с высоким уровнем юридической определенности является одним из ключевых вопросов для проработки в рамках пилотного проекта по внедрению национальной цифровой валюты.

Вопросы о том, имеет ли центральный банк полномочия выпускать ЦВЦБ или может ли ЦВЦБ быть законным платежным средством, затрагивают фундаментальные отношения между деньгами, государством и законом. Данные вопросы имеют практическое значение, так как ЦВЦБ должен иметь прочную правовую основу для широкого применения общественностью. При отсутствии прочной правовой основы выпуск ЦВЦБ создает юридические, финансовые и репутационные риски для центральных банков. Хотя надлежащая разработка правовой базы будет в определенной степени зависеть от особенностей дизайна ЦВЦБ, тем не менее определенные выводы в данной сфере имеются.

В контексте данных вопросов исследователи МВФ проанализировали НПА 174 центральных банков с акцентом на два наиболее важных публично-правовых аспекта ЦВЦБ – правовые основы ЦВЦБ в соответствии с законодательством о центральном банке и его режим в соответствии с законодательством в сфере денежного обращения [\[30\]](#).

### Правовые аспекты различных дизайнов ЦВЦБ

#### Дизайн технологии доступа ЦВЦБ на основе счетов и токенов

Правовой статус счетов в рамках частного и публичного права хорошо разработан и понятен. Цифровые токены, напротив, не имеют продолжительной истории, и их правовой статус в соответствии с публичным и частным правом в настоящее время требует доработки.

Во-первых, ЦВЦБ на основе токенов представляет собой требование к центральному банку. По аналогии с передачей банкнот и монет передача токена равносильна передаче требования. Это то, что отличает банкноты, монеты и ЦВЦБ на основе токенов от денег на счетах и векселей (долговых ценных бумаг), которые переводятся по дебетам и кредитам между текущими счетами наличных средств и счетами ценных бумаг соответственно.

Во-вторых, как для физических, так и цифровых форм токенов держатель должен либо владеть банкнотами/монетами, либо знать пароль, позволяющий распоряжаться валютой. Если владелец потеряет либо банкноты/монеты, либо пароль, он больше не сможет использовать валюту. Тогда как владелец счета при потере пароля все равно сможет распоряжаться средствами до тех пор, пока это лицо сможет подтвердить свою личность организации, подтверждающей учетную запись.

В-третьих, в таксономии обязательств центрального банка ЦВЦБ на основе токенов не является ни деньгами на счетах, ни векселем. В случае, если ЦВЦБ будет выпущена для широкой публики, она будет иметь сходство с банкнотами и монетами, которые также выпускаются для широкого распространения.

<p><b>Доступность для потребителей</b></p> <p><b>Оптовые и розничные ЦВЦБ</b></p>	<p>Некоторые центральные банки рассматривают возможность выпуска ЦВЦБ только для существующих владельцев счетов и участников платежных систем RTGS. В основном это (крупные «клиринговые») банки и государственные органы («оптовая торговля»). Другие центральные банки гораздо шире используют сеть и стремятся предлагать ЦВЦБ широкой публике («розничным»), не предлагая ее оптовым клиентам. Наконец, некоторые центральные банки считают, что их ЦВЦБ должна быть «общего назначения» и доступна как оптовым, так и розничным контрагентам.</p> <p>С юридической точки зрения, это различие уместно в тех случаях, когда ЦВЦБ разработана в виде счета. Законы многих центральных банков ограничивают категории юридических и физических лиц, которые могут открывать подобные счета. Другими важными правовыми вопросами являются правила борьбы с отмыванием денег и законодательство о конкуренции.</p>
<p><b>Подход к реализации архитектуры</b></p> <p><b>Прямой, непрямой и гибридный</b></p>	<p>Отдельные центральные банки рассматривают возможность выпуска ЦВЦБ в прямой или одноуровневой форме: они будут выпускать ЦВЦБ и самостоятельно управлять их обращением. Другие финансовые институты рассматривают возможность выпуска в косвенной двухуровневой форме (также называемой «синтетической»), в соответствии с которой обязательства выдаются коммерческим банком, но полностью обеспечены центральным банком. Гибридная форма будет состоять из прямых требований к центральному банку и посредникам, обрабатывающим платежи.</p> <p>С юридической точки зрения, возникают два важных вопроса. Во-первых, чтобы квалифицироваться как ЦВЦБ, «валюта» должна стать прямой ответственностью центрального банка; это то, что делает ее безрисковой. Обязательства коммерческих банков, даже если они обеспечены 100% денежным депозитом в бухгалтерских книгах центрального банка, не являются обязательством последнего. Во-вторых, в случае ЦВЦБ на основе токенов возникает вопрос о том, позволяет ли и при каких условиях правовая база «вносить» ЦВЦБ в бухгалтерские книги коммерческих банков.</p>
<p><b>Подход к организации технологической инфраструктуры</b></p> <p><b>Централизованный и децентрализованный</b></p>	<p>Центральные банки обсуждают, будут ли переводы ЦВЦБ осуществляться централизованно — как в нынешних RTGS — или децентрализованно, с применением технологии распределенных реестров (DLT). Что касается последнего, то дополнительной переменной станет то, будет ли DLT работать на открытой или закрытой основе. Учитывая влияние, которое может оказать DLT на открытой основе, в том числе потенциально усложняющее способность центрального банка управлять денежной массой, весьма вероятно, что центральные банки выберут DLT закрытого типа. Однако, обсуждения правовых последствий данного выбора все еще ведутся.</p>

Хотя конструктивные особенности имеют определенное юридическое значение, различие между ЦВЦБ на основе учетных записей и токенов имеет наиболее существенные юридические последствия. В связи с этим требуется проработка многих открытых вопросов в контексте ЦТ на основе токенов. Для адекватной оценки юридических различий между текущими счетами и ЦТ на основе токенов, обрабатываемых централизованно или с помощью закрытого DLT, необходимо подчеркнуть юридическое различие между текущими счетами наличных средств и (общими) счетами главной книги (ledger account).

**Текущие счета наличных средств** (cash current account) являются банковским методом и представляют собой особые договорно-правовые отношения между финансовым учреждением и владельцем счета. Следовательно, права и обязанности сторон в основном предусмотрены договорными положениями и условиями, регуливающими учетную запись. Также могут применяться законодательные положения и общие правовые принципы. В большинстве юрисдикций текущие счета наличных средств функционируют на основе взаимного договора римского права: хотя денежные средства, зачисленные на счет, называются «депозитами», однако, финансовое учреждение не обязано хранить данные денежные средства, а лишь имеет право использовать их в дальнейшем. Кредитные остатки на текущих счетах наличности переводятся по дебету и кредиту между счетами.

**Счета главной книги** (ledger account) являются методом бухгалтерского учета, а не договорной концепцией: они отражают финансовое положение отчитывающегося предприятия на основе субсчетов, установленных планом счетов предприятия. Счета главной книги могут представлять собой актив, обязательство, доход или расход. Счета главной книги сами по себе не устанавливаются и не представляют собой юридических отношений между отчитывающимся предприятием и третьей стороной и не создают прав и обязанностей между отчитывающимся предприятием и другими сторонами (но ничто не мешает отчитывающемуся субъекту и третьим лицам вступать в договорные отношения).

Конечным юридическим следствием этого различия является то, что, хотя ЦТ на основе токенов может быть представлен центральным банком на централизованно управляемых счетах главной книги (ledger account), он не является кредитным балансом на текущем счете. Это означает, что между центральным банком и держателем ЦТ на основе токенов не существует договорных отношений за исключением (по общему признанию, очень специфического) требования, включенного в токен, очень похожего на правовой статус банкнот. Тем не менее, эксперты МВФ выработали ряд рекомендаций для центральных банков, рассматривающих цифровые валюты на основе токенов, применимых и в Казахстане.

### **Необходимо внести соответствующие изменения в законодательство о центральном банке**

Отсутствие четкой и надежной правовой основы для выпуска ЦВЦБ на основе токенов и/или счетов влечет целенаправленную реформу законодательства о центральном банке.



Согласно рекомендациям по выпуску ЦВЦБ на основе токенов логично внесение следующих поправок в законодательство о Центробанке:

1. Закон должен описывать четкую функцию «выпуска валюты» в целом, не ограничивая выпуск исключительно в форме банкнот и монет.
2. Соответствующие полномочия по осуществлению этой функции должны быть сформулированы, где это уместно, с четкой ссылкой на выпуск валюты в форме банкнот (и, возможно, монет), а также в форме цифрового токена.

Основным аргументом в пользу введения четкой правовой основы является то, что в зависимости от предполагаемого дизайна данная поправка будет поддерживать более инновационные функции ЦВЦБ (например, ограниченную конфиденциальность и общую доступность).

Для обеспечения правовой основы по выпуску ЦВЦБ на основе счета широкой общественности, в частности, следует внести поправки в законы о центральном банке с расширением конкретных полномочий по открытию текущих счетов. Например, путем упоминания широкой общественности в законе или принятия компетентным органом решений о категориях физических и юридических лиц, которые будут иметь доступ к текущим счетам в бухгалтерских книгах центрального банка.

Применительно к обоим типам ЦВЦБ требуется внимательное рассмотрение формулировки функции платежной системы при ее ограничении межбанковскими платежными системами на предмет оптимальной редакции.

**Необходимо внести соответствующие изменения в законодательные акты, регулирующие и определяющие основы выпуска денег, денежного обращения и денежно-кредитных отношений.**

Вместе с тем, учитывая, что данный процесс затрагивает фундаментальные и концептуальные вопросы правовой политики, требуется тщательный анализ и определение стратегии внесения изменений в законодательные акты соответствующими государственными органами.

В свою очередь, необходимость внесения изменений в законодательные акты, регулирующие выпуск денег, денежное обращение и денежно-кредитные отношения исходит также из задачи по юридическому приравниванию ЦВЦБ на основе токенов с банкнотами. Согласно исследованиям МВФ, странам рекомендуется сначала рассмотреть вопрос о том, следует ли и можно ли предоставить этому типу ЦВЦБ статус законного платежного средства. Одним из вариантов в этом отношении является ограничение данного статуса закрытой категорией определенных юридических лиц (государство, государственные органы и торговцы за пределами определенного размера и/или фирмы с разрешенной деятельностью, такие как банки).



В качестве следующего шага странам рекомендуется анализ частно-правовой классификации ЦВЦБ на основе токенов и вопрос о том, следует ли предоставлять этой новой форме денег привилегии в соответствии с частным правом (в частности, с целью содействия ее обращению). В качестве третьего шага властям предлагается пересмотреть определения преступлений, связанных с киберпреступностью с тем, чтобы они четко охватывали преступления, связанные с киберпреступностью против ЦВЦБ.

В свою очередь, если речь идет о ЦВЦБ на основе счетов, то на данном этапе не стоит задача по внесению изменений в законодательство, регулирующее денежное обращение и денежно-кредитные отношения.

Следует отметить, что возможное внедрение ЦТ затронет регуляторные аспекты, связанные с Законом «О Национальном Банке Республики Казахстан», Законом «О банках и банковской деятельности», налоговым законодательством, частным правом (включая имущественное), договорным правом, законодательством о платежах и платежных системах, законодательством о реабилитации и банкротстве, законом о персональных данных и их защите, международным частным правом. Кроме того, необходимо тщательно проработать эффективное внедрение системы ПОД/ФТ. Данный перечень может быть неисчерпывающим и будет дополнен по результатам дальнейшего исследования.

### Открытые вопросы для дальнейшей проработки

Наименование	Аспекты дальнейшей проработки
<b>Определение ЦТ</b>	<p>Определение статуса и роли ЦТ как новой формы денег, в том числе изменение текущих НПА в части регулирования процентных ставок при осуществлении денежно-кредитной политики.</p> <p>Установление ЦТ в качестве официальной денежной единицы, обязательной для осуществления функции средства платежа.</p> <p>Определение ЦТ как отдельного вида безналичных денежных средств.</p>
<b>Роли участников и НБРК</b>	<p>Определение регулирования ролей участников: права и обязанности участников цифровой платформы.</p> <p>Определение полномочий НБРК как оператора цифровой платформы: права НБРК по осуществлению банковских операций с применением ЦТ как с кредитными организациями, так и юридическими и физическими лицами.</p> <p>Распределение ответственности за деятельность информационной системы, в рамках которой происходит обращение ЦВЦБ.</p>
<b>Требования к участникам</b>	<p>Определение критериев и требований к финансовым игрокам, в том числе проработка требований к ликвидности, операционных правил распределения и лимитов по использованию ЦТ для ограничения перетока капитала из средств коммерческих банков.</p> <p>Проработка требований к KYC-проверкам на стороне участников финансового рынка, определение критериев и требований к AML и CFT-проверкам с учетом конфиденциальности и возможности анонимных платежей.</p>
<b>Безопасность</b>	<p>Проработка требований и критериев к защите персональных данных пользователей, составляющих банковскую тайну, и распределение ответственности между участниками.</p>
<b>Использование ЦТ</b>	<p>Проработка правового режима использования ЦТ в гражданских правоотношениях, в т.ч. изменение положений законодательства, регулирующих сферу расчетов и установление особенностей исполнения денежных обязательств с применением ЦТ.</p> <p>Проработка изменений в сфере налогового и бюджетного законодательства, изменение режимов обращения взыскания на имущество (в т.ч. определение особенностей распоряжения цифровым кошельком в рамках отношений, связанных с банкротством).</p>
<b>Технические требования</b>	<p>Проработка технических стандартов и требований к функционированию ЦТ, в том числе – к интероперабельности, программируемости, безопасности, масштабируемости.</p> <p>Выбор модели доступа к ЦВЦБ в зависимости от правовых отношений и проработка соответствующего регулирования (прямой доступ, гибридный через поставщика платежных/технических услуг, косвенный через посредников).</p>


Помимо проработки возможностей применения в розничных платежах, НБРК планирует также рассмотреть потенциал использования ЦТ для межбанковских расчётов и платежей между организациями.

Использование платформы ЦТ может позволить существенно повысить эффективность взаиморасчетов между игроками рынка, что достигается за счёт обеспечения доверия в системе распределенных реестров. Возможность передавать стоимость напрямую, без использования посредников, может существенно упростить взаиморасчеты между участниками рынка, например в цепочках поставок или для мгновенных финальных расчётов на рынке ценных бумаг.

Помимо улучшения эффективности и снижения издержек в существующих сферах межбанковских расчетов ЦТ также может позволить реализовать новые эффективные инструменты для участников рынка: в частности, токенизация различных видов активов позволяет использовать ЦВЦБ для мгновенных низкорисковых расчётов в режиме DvP (поставка против платежа).

Возможности ЦТ в рамках трансграничных платежей будут в дальнейшем исследованы в партнерстве с международными организациями и другими центральными банками.

### Потенциал развития трансграничных платежей с помощью ЦВЦБ

 <p><b>Актуальные проблемы трансграничных платежей</b></p>	<p><b>Трансграничные сценарии</b></p>	<p><b>Модели интероперабельности/совместимости</b></p>
<ul style="list-style-type: none"> <li>• Фрагментированные и усеченные данные</li> <li>• Сложный процесс комплаенс-проверок</li> <li>• Ограниченные часы работы</li> <li>• Устаревшие технологические платформы</li> <li>• Длинные цепочки транзакций</li> <li>• Затраты на финансирование</li> <li>• Слабая конкуренция</li> </ul>	<p>Нет ограничений на трансграничное использование</p> <p>Скоординированный трансграничный доступ к внутренним ЦВЦБ</p> <p>Соглашения о мульти-ЦВЦБ (mCBDC)</p>	<p><b>Модель 1</b> Совместимые системы ЦВЦБ</p> <p><b>Модель 2</b> Взаимосвязанные системы ЦВЦБ</p> <p><b>Модель 3</b> Единая система для мульти-ЦВЦБ (mCBDC)</p>
<p><b>Потенциальные преимущества при использовании ЦВЦБ</b></p>	<p><b>Потенциальные риски</b></p>	
<ul style="list-style-type: none"> <li>• Меньше посредников</li> <li>• Повышенная эффективность</li> <li>• Улучшенная интеграция</li> <li>• Повышенная техническая совместимость</li> <li>• Повышенная безопасность</li> <li>• Снижение трансграничных и кросс-валютных рисков</li> </ul>	<p>Микрофинансовые, операционные и киберриски</p> <p>Макрофинансовые риски (международные утечки, финансовая стабильность, денежная политика)</p>	

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

Следующие шаги

стр. **90-92**



Реализация пилотного проекта по внедрению ЦТ в 2021 году позволила заложить фундамент для базовой архитектуры национальной цифровой валюты в Казахстане, определив ключевые параметры дизайна, технологических подходов, а также предварительных моделей для оценки экономических аспектов и соответствующей регуляторной базы. НБРК отмечает высокий вклад в вовлечение участников рынка и экспертного сообщества для прогресса исследования.

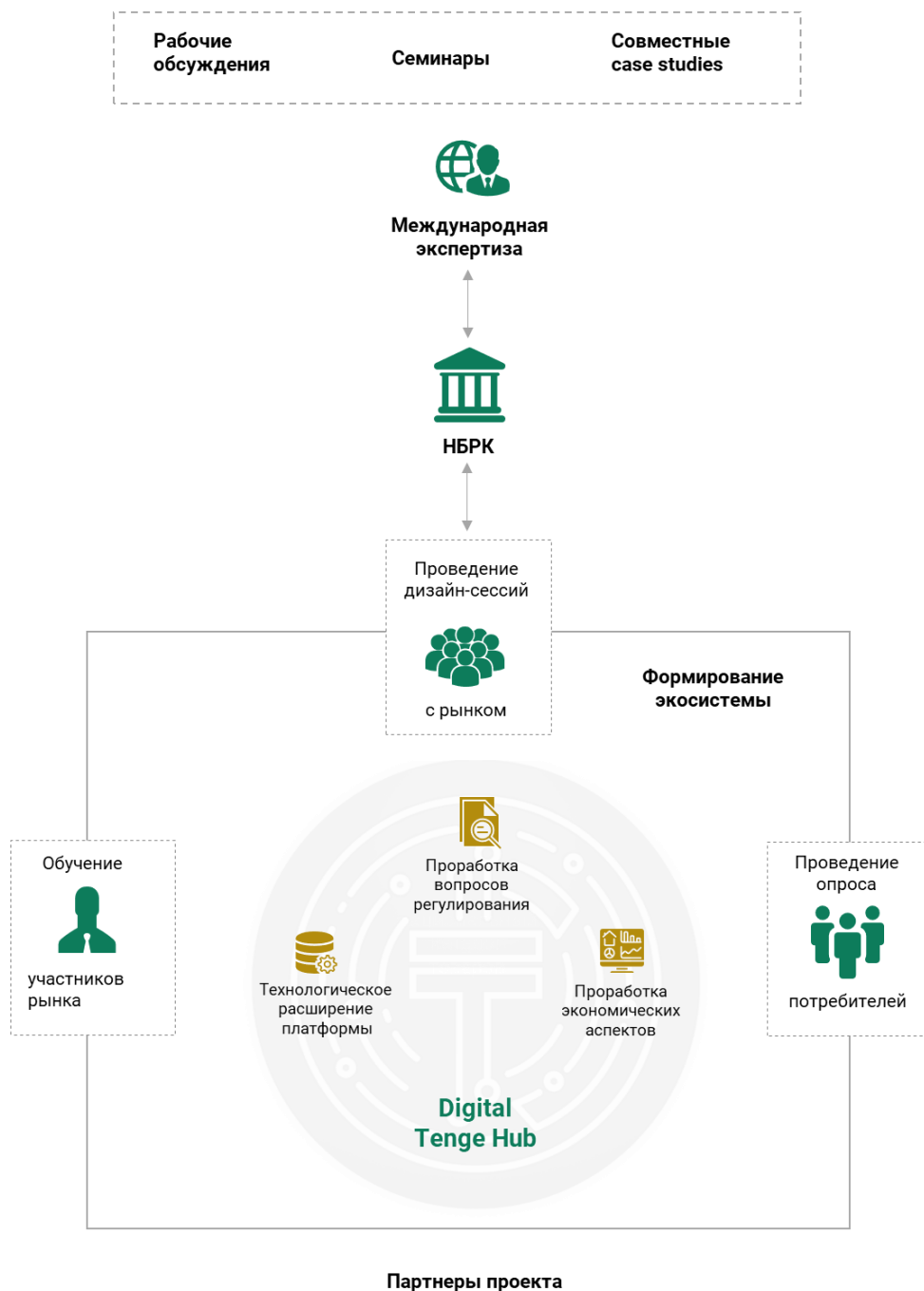
По итогам проведенной совместно с международными партнерами (МВФ, БМР, коллаборативными исследовательскими институтами) работе по оценке результатов исследования текущего года, а также анализу аналогичных работ центральных банков зарубежных государств НБРК выделяет следующие стратегические вехи дальнейшего исследования:

- 1. Создание коллаборативной площадки Digital Tenge Hub** для проведения дизайн-сессий с участниками рынка и экспертным сообществом, а также создания комплексного инструмента для подключения и обучения работе с пилотной платформой ЦТ по принципу «единого окна». Особое внимание НБРК в рамках данной площадки будет уделено вопросам создания перспективной экосистемы ЦТ, в том числе, за счет содействия в создании сервисов на базе ЦТ для участников рынка. Digital Tenge Hub станет ключевой платформой для вовлечения рынка и экспертов в выработку принятия решения о внедрении ЦТ.
- 2. Проведение комплексного экономического исследования**, в том числе с использованием качественных и количественных методов, включая оценку потребительских паттернов использования платежных инструментов, качественного и количественного спроса на перспективный ЦТ, а также воздействия возможного внедрения на ключевые экономические параметры. Совместно с участниками рынка будут детально изучены эффекты на финансовую стабильность и бизнес-модели игроков платежного рынка, а также выработаны меры по контролю за соответствующими рисками. Будут разработаны экономические аспекты дизайна ЦТ, включая модель его учета.
- 3. Расширение функциональности пилотной платформы ЦТ** параллельно с проработкой ряда технологических вопросов, в том числе аспектов масштабируемости/производительности, информационной безопасности, интероперабельности с действующей платежной инфраструктурой и т.д. В ограниченном периметре вместе с участниками рынка и инфраструктурными игроками (в том числе, международные платежные системы) будет протестирована функциональность ключевых сценариев использования платформы ЦТ.
- 4. Проработка регуляторных аспектов внедрения ЦТ** позволит выработать перечень конкретных рекомендаций для юридической однозначности и создания сбалансированной среды для функционирования ЦТ. Будут определены необходимые изменения для закрепления терминологического аппарата; роли, права и обязанности участников оборота; регуляторные механизмы для контроля возможных рисков; аспекты ПОД/ФТ и т.д.

НБРК обеспечит разработку итоговой модели принятия решения о внедрении ЦТ, а также презентацию промежуточных итогов исследования и обсуждение со всеми заинтересованными сторонами в июле 2022 года.

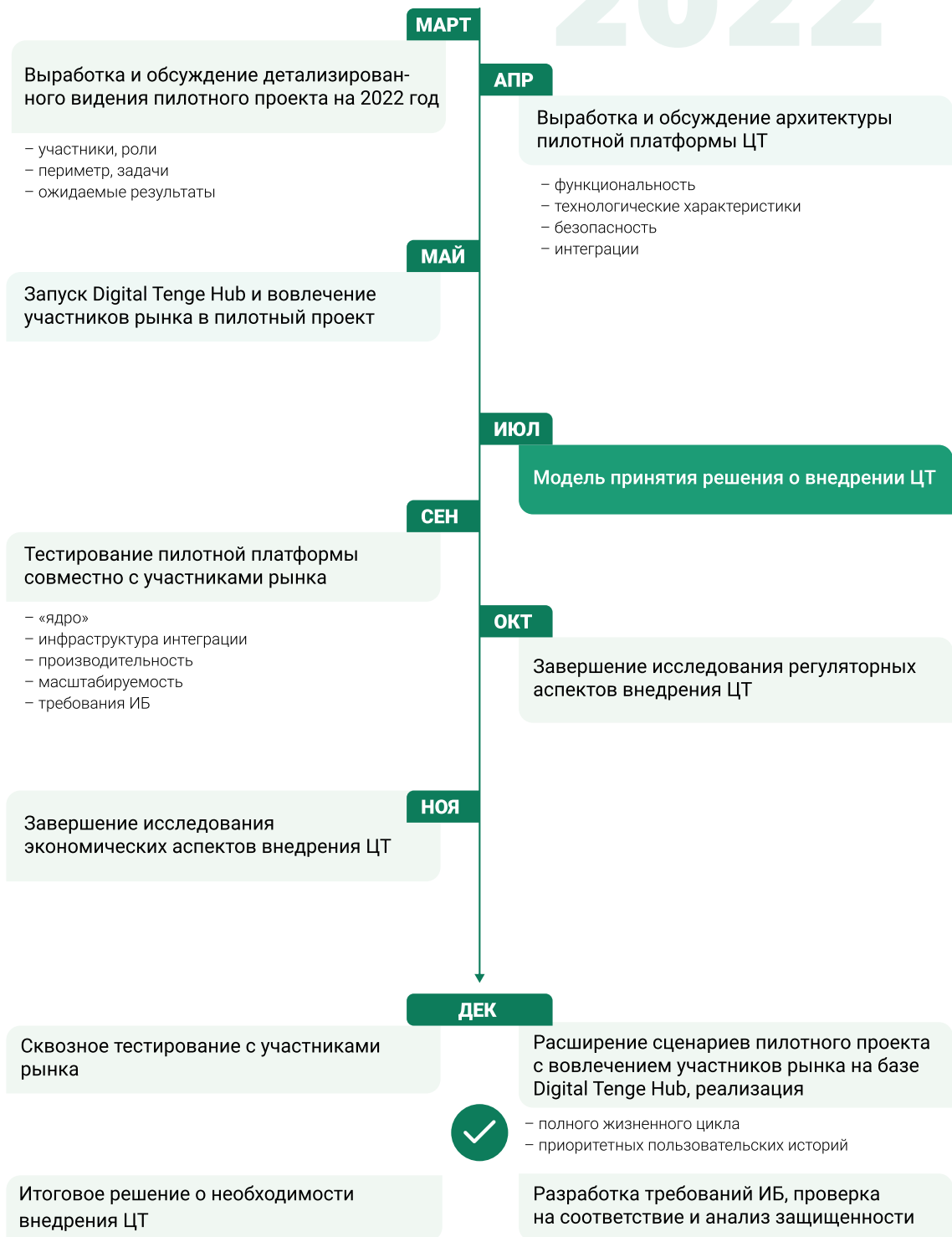
Решение о необходимости внедрения ЦТ будет принято в декабре 2022 года с учетом финальных итогов комплексного исследования на базе разработанной модели.

## Подход к изучению ЦТ в 2022 году





# ЯНВАРЬ 2022



Национальный Банк обеспечит активное вовлечение и регулярные обсуждения промежуточных результатов проекта со всеми заинтересованными сторонами в течение 2022 года

## Отзывы экспертов



**Профессор Джамизель Шейх**

**Основатель CBDC Think Tank  
(Аналитического Центра ЦВЦБ)**

**Автор «Mastering Corda &  
The Decentralized Finance  
Phenomenon»**

Проект «Цифровой тенге» показывает пример открытого и взвешенного подхода во внедрении инноваций в финансовой отрасли. С появлением криптовалют и стейблкоинов еще больше возрос глобальный спрос на новые способы представления, хранения и обмена ценности. Центральные банки по-разному реагируют на этот тренд – некоторые заняли выжидательную позицию, проводя лишь теоретические исследования, другие проводят серии экспериментов, а некоторые страны уже перешли к стадии полноценного внедрения или запуска своих цифровых валют. Проект Национального Банка Казахстана – цифровой тенге – это вдохновляющий, впечатляющий шаг в этом направлении. Я особенно восхищен результатами экспериментов по реализации возможностей оффлайн-платежей, программируемости и регулируемой анонимности цифрового тенге. Эти три свойства являются одними из наиболее сложных задач и ставят наиболее головомомные вопросы в сфере разработки ЦВЦБ. Идею ЦВЦБ часто отвергают из-за ассоциации с инструментом контроля за населением, однако НБРК успешно продемонстрировал, что это не обязательно должно быть так.

Программируемость цифрового тенге, например, в случае распределения средств – темы моих исследований в последние несколько лет (я стал автором термина «disburse» для платежей в США), показывает, что НБРК рассматривает широкий спектр применений своей цифровой валюты. Хотя документ дает ответы на многие вопросы, тем не менее все еще немало других остаются открытыми, и я с нетерпением жду ответы на них в будущем от НБРК, в том числе на вопросы о том, как будут работать «легкие клиенты», какие требования будут предъявляться к пропускной способности, масштабируемости и доступности платформы для пользователей. В документе проделана большая отличная работа по объяснению интересных решений, проработанных в пилоте, включая использование ключа расходов, детальный подход к сценариям и анализ влияния цифрового тенге на показатели монетарной статистики. Также глубоко проработаны регуляторные аспекты и последствия внедрения цифрового тенге.

Доклад может служить ориентиром для других центральных банков, неправительственных организаций, ученых, энтузиастов цифровых- и криптовалют и вообще всех, кто просто хочет получить представление о том, как ЦВЦБ может быть внедрена такой одаренной командой, как у НБРК.

## Отзывы экспертов



**Вилли Лим**

**Руководитель отдела  
глобальных консультаций по  
цифровым валютам и рынкам  
капитала, R3**

Проект «Цифровой тенге» предоставил Национальному Банку Республики Казахстана возможность изучить целесообразность и применение ЦВЦБ общего назначения в Казахстане. В условиях стремительного перехода мировой экономики к цифровой экономике возрастает значение дефицита времени для определения приоритетности, потребности в платежном инструменте, выпущенном доверенным лицом, способствующем всеобщему доступу и стимулирующем инновации. Именно таково видение цифрового тенге в контексте продолжающегося развития в Казахстане цифровой экономики как внутри страны, так и на международном уровне, укрепления его также в качестве центра роста и инноваций в Центральной Азии.

Цифровой тенге позволил НБРК проанализировать такие инновационные функции как программируемые деньги, автономные платежи и экосистему, которые может обеспечить цифровой тенге. Такие функции позволяют эффективно реализовывать важные сценарии использования, например, касающихся цифровой грамотности, предоставления эффективных социальных платежей и аналитики в режиме реального времени, которые способствуют точному планированию ключевых макроэкономических показателей. Функция предоставления аналитики в режиме реального времени особенно интересна, поскольку позволяет директивным органам точно планировать и внедрять различные инструменты политики на основе точных макроэкономических показателей в целевых секторах.

Я выражаю благодарность НБРК за подготовку этого превосходного отчета. В документе содержатся ответы на такие важные вопросы, как последствия регулирования, применение DLT для снижения риска узловых точек отказа и применение программируемости. Программируемость особенно интересна, поскольку она способна повысить эффективность и устранить пробелы в выявлении мошенничества, а также способствовать внедрению инновационных услуг, востребованных пользователями.

Успешное завершение Фазы 1, кульминацией которой является данный отчет, закладывает основу для Фазы 2, позволяя НБРК реализовать целевые сценарии использования, отвечающие потребностям Казахстана. Я поздравляю всю команду НБРК с этим новаторским достижением.

# Список литературы

1. Mngomezulu, Z., Rimer, S., Ouahada, K., Ndjongue, A. (2017). A review of Bluetooth and NFC for financial applications. In Sixth International Conference on Advances in Computing, Control and Networking-ACCN 2017 (pp. 48-51). <https://ujcontent.uj.ac.za/vital/access/services/Download/uj:24322/SOURCE1>
2. Igboanusi, I. S., Dirgantoro, K. P., Lee, J. M., & Kim, D. S. (2021). Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture. ICT Express <https://www.sciencedirect.com/science/article/pii/S2405959521000928>
3. Omilabu, A. A., Olusanya, O. O., Adebare, A. A., Ibitowa, F., & Longe, O. B. (2017). Comparative Analysis of Wi-Fi, Bluetooth & Xender Wireless Technology Applications. Computing, 8(4). [https://www.researchgate.net/publication/349477834\\_Done\\_3\\_CISDI](https://www.researchgate.net/publication/349477834_Done_3_CISDI)
4. Noether, S., & Mackenzie, A. (2016). Ring confidential transactions. Ledger, 1, 1-18. <http://ledger.pitt.edu/ojs/ledger/article/view/34>
5. Metere, R., & Dong, C. (2017, August). Automated cryptographic analysis of the pedersen commitment scheme. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 275-287). Springer, Cham. [https://link.springer.com/chapter/10.1007/978-3-319-65127-9\\_22](https://link.springer.com/chapter/10.1007/978-3-319-65127-9_22)
6. Opare, E. A., & Kim, K. (2020). A compendium of practices for central bank digital currencies for Multinational financial infrastructures. IEEE Access, 8, 110810-110847 <https://ieeexplore.ieee.org/abstract/document/9115606>
7. Klein, M., Gross, J., & Sandner, P. (2020). The Digital Euro and the Role of DLT for Central Bank Digital Currencies. FSBC Working Paper, Frankfurt School Blockchain Centre [https://researchgate.net/publication/341354711\\_The\\_Digital\\_Euro\\_and\\_the\\_Role\\_of\\_DLT\\_for\\_Central\\_Bank\\_Digital\\_Currencies](https://researchgate.net/publication/341354711_The_Digital_Euro_and_the_Role_of_DLT_for_Central_Bank_Digital_Currencies)
8. Scorer, S. (2017). Central Bank Digital Currency: DLT, or not DLT? That is the question. <https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/>
9. R3 Sandbox for Digital Currencies. <https://www.r3.com/digital-currency-sandbox/>
10. Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., ... & Zhang, F. (2020). Design choices for central bank digital currency: Policy and technical considerations (No. w27634). National Bureau of Economic Research <https://nber.org/papers/w27634>
11. DTCC, What we learned from our DLT capability study. A Q&A with DTCC's Jennifer Peve. <https://www.dtcc.com/dtcc-connection/articles/2018/november/08/what-we-learned-from-our-dlt-capability-study>
12. Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. Ict Express, 7(2), 229-233. <https://www.sciencedirect.com/science/article/pii/S2405959520301909>
13. Han, R., Shapiro, G., Gramoli, V., & Xu, X. (2020). On the performance of distributed ledgers for internet of things. Internet of Things, 10, 100087. <https://www.sciencedirect.com/science/article/abs/pii/S2542660518300416>
14. Monetary Authority of Singapore and Accenture, Project Ubin (2016 – 2021) <https://www.mas.gov.sg/schemes-and-initiatives/project-ubin>
15. Accenture, The (R)evolution of Money: Blockchain Empowered Digital Currencies (2017) [https://www.accenture.com/t20171116T025715Z\\_w\\_us-en\\_acnmedia/PDF-63/Accenture-Evolution-Money-Blockchain-Digital-Currencies.pdf](https://www.accenture.com/t20171116T025715Z_w_us-en_acnmedia/PDF-63/Accenture-Evolution-Money-Blockchain-Digital-Currencies.pdf)
16. Accenture, The (R)evolution of Money II: Blockchain Empowered CBDC (2020) <https://www.accenture.com/us-en/insights/blockchain/evolution-money>
17. Accenture, Connecting ecosystems: Blockchain integration (2018) <https://accenture.com/us-en/insights/blockchain/integration-ecosystems>

## Список литературы

18. Accenture and DTCC, Governing DLT Networks, DLT Governance for Private Permissioned Networks (2019) [https://www.accenture.com/\\_acnmedia/accenture/redesign-assets/dotcom/documents/global/2/accenture-governing-dlt-networks.pdf](https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/global/2/accenture-governing-dlt-networks.pdf)
19. ECB and Accenture, Exploring anonymity in central bank digital currencies with European Central Bank (2019) <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf>
20. Digital Dollar Foundation and Accenture, The Digital Dollar Project (2020) [http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper\\_vF\\_7\\_13\\_20.pdf](http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf)
21. Riksbank and Accenture, The Riksbank's e-krona pilot (2018 – 2021) <https://www.riksbank.se/globalassets/media/rappporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf>
22. Corda. An analysis of Ethereum's recent chain split. <https://www.corda.net/blog/an-analysis-of-ethereums-recent-chain-split/>
23. Bickers K. Blockstream Sponsors Federated E-Cash as a Bitcoin Scaling Technology. <https://medium.com/blockstream/blockstream-sponsors-federated-e-cash-as-a-bitcoin-scaling-technology-637ba05de7b3>
24. World Economic Forum: Digital Currency. Governance Consortium. White Paper Series. Compendium Report, Nov 2021 [https://www3.weforum.org/docs/WEF\\_Digital\\_Currency\\_Governance\\_Consortium\\_White\\_Paper\\_Series\\_2021.pdf](https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf)
25. Global CBDC Challenge Problem Statements organized by Monetary Authority of Singapore, November 2021 [https://tribex.co/wp-content/uploads/2021/06/Global\\_CBDC\\_Challenge\\_Problem\\_Statements.pdf](https://tribex.co/wp-content/uploads/2021/06/Global_CBDC_Challenge_Problem_Statements.pdf)
26. Auer R., Cornelli G., Frost J. Rise of the central bank digital currencies: drivers, approaches and technologies. <https://www.bis.org/publ/work880.htm>
27. BIS: Central bank digital currencies: foundational principles and core features. Report # 1 in a series of collaborations from a group of central banks. [https://www.bis.org/publ/othp33\\_summary.pdf](https://www.bis.org/publ/othp33_summary.pdf)
28. G7 United Kingdom 2021: Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1025235/G7\\_Public\\_Policy\\_Principles\\_for\\_Retail\\_CBDC\\_FINAL.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf)
29. BIS Annual Economic Report 2021 <https://www.bis.org/publ/arpdf/ar2021e3.pdf>
30. Bossu W., Itatani M., Margulis C., Rossi A., Weenink A., Yoshinaga A. Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>
31. ЦТ. Доклад для публичных обсуждений. НБРК. Май 2021 г. <https://nationalbank.kz/ru/page/cifrovoy-tenge-pilotnyy-proekt>
32. Реестр платежных систем (2020) <https://www.nationalbank.kz/ru/news/reestr-platezhnyh-sistem>
33. Система межбанковского клиринга <https://www.nationalbank.kz/ru/news/sistema-mezhbankovskogo-kliringa>
34. СМЭП и СМП. <https://www.kisc.kz/catalog/smep>
35. Статистика прохождения платежей через СМЭП. <https://www.kisc.kz/catalog/177>
36. Платежные карточки и электронные банковские услуги [11/2021] <https://www.nationalbank.kz/ru/news/elektronnye-bankovskie-uslugi?page=1>