ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 51.77

ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ ПРИ ПРОВЕДЕНИИ ОФЛАЙН-ТРАНЗАКЦИЙ В ЦИФРОВЫХ ВАЛЮТАХ ЦЕНТРАЛЬНЫХ БАНКОВ

Солодуха Мария Алексеевна,
магистрант, Финансовые технологии и аналитика, Московский физико-технический университет, г. Москва, Российская Федерация.
E-mail: mari_solod@mail.ru

Аннотация

Развитие цифровых валют центральных банков (ЦВЦБ) сопровождается необходимостью обеспечения устойчивости платежной инфраструктуры, в том числе в условиях отсутствия сетевого подключения. В этой связи особую значимость приобретает реализация офлайн-транзакций. В статье проводится системный анализ технологий передачи данных, применимых для офлайн-платежей, с акцентом на технологии ближней связи. Выделены ключевые требования к офлайн-транзакциям, проанализированы архитектурные решения и возникающие компромиссы, а также рассмотрены практические кейсы реализации. На основе сравнительного анализа предложены рекомендации по выбору технологических решений.

Ключевые слова: ЦВЦБ, цифровые валюты центральных банков, офлайн-транзакции, архитектура.

DATA TRANSMISSION TECHNOLOGIES FOR CONDUCTING OFFLINE TRANSACTIONS IN CENTRAL BANK DIGITAL CURRENCIES

Maria A. Solodukha,
master's Student, Financial Technology and Analytics, Moscow Institute of Physics and Technology, Moscow, Russian Federation.
E-mail: mari_solod@mail.ru

ABSTRACT

The development of central bank digital currencies (CBDCs) is accompanied by the need to ensure the resilience of payment infrastructure, including in conditions of no network connectivity. In this regard, the implementation of offline transactions becomes particularly important. This paper provides a systematic analysis of data transmission technologies applicable to offline payments, with a focus on near-field communication technologies. The study identifies key requirements for offline transactions, analyzes architectural solutions and the resulting trade-offs, and examines practical implementation cases. Based on a comparative analysis, recommendations for the selection of technological solutions are proposed.

Keywords: CBDC, central bank digital currencies, offline transactions, architecture.

Введение

Цифровые валюты центральных банков (ЦВЦБ), представляющие третью форму национальной валюты, выпускаемой и гарантируемой центральным банком, становятся важным направлением развития платежных систем. Более 100 стран, на долю которых приходится около 98% мирового ВВП, ведут исследования или реализуют пилотные проекты в данной области [1]. Важным требованием к розничным ЦВЦБ является обеспечение непрерывности платежей, включая возможность проведения офлайн-транзакций.

Необходимость офлайн-функциональности обусловлена зависимостью современных платежных систем от интернет-инфраструктуры. В отличие от онлайн-платежей, офлайн-транзакции выполняются без доступа к централизованному реестру, что увеличивает риски двойного расходования, усложняет валидацию операций и соблюдение требований ПОД/ФТ [2]. Существенное влияние на решение этих задач также оказывает выбор технологий передачи данных между устройствами пользователей.

Существующие исследования в основном сосредоточены на архитектуре и безопасности ЦВЦБ, тогда как технологии передачи данных рассматриваются изолированно, без учета их взаимосвязи с требованиями к системе [3][4]. В результате отсутствует интегральный подход к их выбору.

Таким образом, разработка офлайн-решений в рамках ЦВЦБ предполагает необходимость балансирования между требованиями безопасности, уровнем контроля со стороны регулятора и удобством для пользователей. В связи с этим, рассматриваются следующие исследовательские вопросы:

Какие технологии передачи данных применимы для реализации офлайн-транзакций в ЦВЦБ?

Какие компромиссы возникают при использовании различных технологических решений?

Каким образом выбрать оптимальное решение с учетом требований системы и условий эксплуатации?

Целью работы является систематизация технологий передачи данных для офлайн-транзакций в ЦВЦБ, а также формирование обоснованных рекомендаций по их выбору с учетом требований к безопасности, приватности и устойчивости системы.

Требования к офлайн-транзакциям в ЦВЦБ

Функционирование офлайн-транзакций в ЦВЦБ предполагает выполнение ряда требований, сформулированных в исследованиях международных организаций и центральных банков. Анализ отчетов Банка международных расчетов (BIS) [3][4], Международного валютного фонда (IMF) [2] показывает, что они формируются вокруг необходимости балансирования между автономностью, безопасностью, приватностью и централизованным контролем. Данные требования взаимосвязаны и часто противоречат друг другу, что требует учета компромиссов при проектировании.

Обобщение требований представлено в таблице 1.

Таблица 1. Ключевые требования к офлайн-транзакциям в ЦВЦБ

Требование	Содержание
Устойчивость	Обеспечение непрерывной работы системы (24/7), функционирование без подключения к сети, отсутствие единой точки отказа
Инклюзивность	Доступность системы для различных групп пользователей и устройств, включая смартфоны, смарт-карты и аппаратные решения
Приватность	Обеспечение уровня анонимности, сопоставимого с наличными средствами, при сохранении механизмов соответствия требованиям ПОД/ФТ
Безопасность	Защита от мошенничества, двойного расходования и киберугроз, обеспечение целостности транзакций
Синхронизация	Обеспечение корректной передачи и согласования транзакций с центральной системой после восстановления соединения
Ограничение рисков	Минимизация потенциального ущерба в условиях невозможности полного контроля офлайн-транзакций, включая использование лимитов и временных ограничений

Представленные требования определяют архитектуру системы. Так, обеспечение автономности приводит к необходимости реализации офлайн-кошельков, требования безопасности — к переносу управления криптографическими ключами на сторону клиента, а невозможность полного предотвращения двойного расходования — к введению лимитов и временных ограничений.

Ключевое значение имеют системные противоречия между требованиями, требующие управляемого компромисса:

приватность vs контроль (ПОД/ФТ): повышение анонимности ограничивает мониторинг и требует усиления механизмов ограничения рисков;

автономность vs безопасность: отсутствие проверки транзакций в реальном времени увеличивает риск двойного расходования и требует компенсирующих мер;

безопасность vs инклюзивность: использование сложных криптографических и аппаратных решений повышает защиту, но снижает доступность системы.

Таким образом, проектирование офлайн-транзакций в ЦВЦБ не предполагает универсального решения и требует адаптации архитектуры к условиям эксплуатации и регулирования. Ключевым элементом такого подхода является осознанное управление компромиссами, прежде всего между приватностью и требованиями комплаенса, а также между безопасностью и удобством использования.

Технологии передачи данных

В реализации офлайн-транзакций в ЦВЦБ ключевую роль играют технологии передачи данных, обеспечивающие прямое взаимодействие между устройствами. Их выбор определяется характеристиками, такими как безопасность, скорость, радиус действия и ограничения применимости, а также степенью соответствия требованиям, рассмотренным ранее.

К основным применимым технологиям относятся Bluetooth Low Energy (BLE), NFC, QR-коды и Wi-Fi Direct [5][6].

Для обоснованного выбора технологий используется многокритериальный подход, учитывающий безопасность, инклюзивность, время установления соединения, скорость

передачи данных и радиус действия. С учетом приоритетности требований критерии были взвешены, чтобы распределение отражало доминирующую роль безопасности и доступности по сравнению с характеристиками производительности канала. Оценка технологий выполнена по шкале от 0 до 1, где 1 соответствует наилучшему значению по соответствующему критерию и представлена в таблице ниже.

Таблица 2. Сравнительная оценка технологий передачи данных

Технология	Безопасность (0,4)	Инклюзивность (0,3)	Время установления соединения (0,1)	Скорость передачи данных (0,1)	Радиус действия (0,1)	Итоговый балл
Bluetooth	0,7	0,9	0,8	0,6	0,8	0,77
NFC	0,9	0,5	1	0,3	0,2	0,65
QR-коды	0,4	1	0,4	0,2	1	0,66
Wi-Fi Direct	0,6	0,6	0,3	1	0,7	0,62

Bluetooth обеспечивает сбалансированное сочетание характеристик, включая поддержку P2P-взаимодействия, достаточный радиус действия и широкую распространенность, что делает его наиболее предпочтительным для офлайн-платежей. При этом его использование требует дополнительных мер безопасности, включая криптографическую защиту и применение защищенных сред выполнения.

NFC обеспечивает высокий уровень безопасности и быстрое установление соединения, однако ограниченный радиус действия и слабая поддержка P2P снижают его универсальность. QR-коды характеризуются высокой доступностью и минимальными требованиями к устройствам, но ограничены объемом передаваемых данных и уровнем безопасности, что определяет их вспомогательную роль.

Wi-Fi Direct и аналогичные решения обеспечивают высокую скорость передачи данных, однако их применение ограничено высокой энергоемкостью, сложностью настройки и недостаточной кроссплатформенной совместимостью.

Таким образом, ни одна технология не удовлетворяет всем требованиям одновременно, что подтверждает необходимость комбинированного подхода. В частности, Bluetooth целесообразно использовать в качестве основной технологии передачи данных, дополняя его QR-кодами для повышения инклюзивности, тогда как другие технологии применимы в ограниченных сценариях.

Архитектурные решения и компромиссы

Архитектура офлайн-транзакций в ЦВЦБ формируется под влиянием требований к системе и ограничений технологий передачи данных. В отличие от традиционных платежных систем, офлайн-транзакции выполняются без обращения к центральной инфраструктуре, что требует перераспределения функций и введения дополнительных механизмов контроля.

Базовым архитектурным выбором является модель учета. Account-based подход основан на изменении состояния счетов клиентов, тогда как token-based модель предполагает передачу цифровых токенов и проверку их подлинности, что лучше соответствует требованиям автономности и ближе к логике наличных средств.

Независимо от модели учета, офлайн-транзакции требуют разделения средств на онлайн- и офлайн-кошельки. Онлайн-кошелек синхронизирован с центральной системой, тогда как офлайн-кошелек представляет изолированную область с ограниченным объемом средств для офлайн-операций. Такое разделение позволяет локализовать риски, связанные с отсутствием централизованной проверки, и упрощает последующую синхронизацию,

обеспечивается баланс между автономностью офлайн-платежей и контролируемостью системы.

Криптографическая защита реализуется на стороне пользователя за счет использования цифровых подписей и локального хранения ключей. Для их защиты применяются изолированные среды выполнения (TEE), позволяющие выполнять критические операции в защищенной области и предотвращать компрометацию ключевой информации. При этом даже при использовании криптографических механизмов, полное устранение рисков при проведении офлайн-транзакций невозможно. Основным инструментом снижения рисков является система ограничений, включающая лимиты на объем средств, сумму транзакций, длину цепочки операций и время использования офлайн-режима.

Технологии передачи данных оказывают существенное влияние на архитектуру, определяя параметры транзакционной модели. В частности, ограниченный объем передаваемых данных (например, в QR-кодах) снижает допустимую длину цепочки транзакций, тогда как технологии с поддержкой устойчивого P2P-взаимодействия (Bluetooth) обеспечивают более гибкие сценарии передачи средств. Таким образом, технологии передачи данных выступают не только средством передачи информации, но и фактором, определяющим архитектурные ограничения системы.

Таблица 3. Взаимосвязь требований, архитектурных решений и технологий передачи данных

Требование	Архитектурное решение	Наиболее применимые технологии передачи данных
Устойчивость	Офлайн-кошельки; автономное выполнение транзакций	Bluetooth (BLE) – поддержка стабильного P2P-взаимодействия
Инклюзивность	Поддержка различных устройств и сценариев	QR – максимальная доступность (требуется только камера) BLE – широкая поддержка на современных смартфонах
Приватность	Локальное выполнение операций; отложенный контроль	BLE, NFC – прямой обмен между устройствами без участия третьих сторон
Безопасность	Хранение ключей на устройстве; TEE; цифровые подписи	NFC – высокий уровень защиты за счет малого радиуса; BLE – требуется реализация дополнительных механизмов шифрования
Синхронизация	Синхронизация данных; передача журналов транзакций	Не участвуют в синхронизации с централизованной системой
Ограничение рисков	Лимиты; разделение кошельков; ограничение автономности	Реализация на уровне архитектуры

В целом архитектура офлайн-транзакций формируется как результат согласования требований и технологических ограничений. Основные элементы – модель учета,

разделение кошельков, локальная криптография и система лимитов – направлены на обеспечение устойчивости, безопасности и контролируемости системы.

Проектирование осуществляется в условиях системных компромиссов: повышение автономности увеличивает риски, усиление безопасности может снижать доступность, а повышение приватности ограничивает возможности контроля. В результате архитектура должна обеспечивать баланс между указанными требованиями.

Выводы

В работе рассмотрены технологии передачи данных для офлайн-транзакций в ЦВЦБ и их взаимосвязь с архитектурными решениями. Показано, что выбор технологий должен осуществляться в контексте требований к безопасности, автономности, приватности и инклюзивности.

К основным технологиям относятся Bluetooth, NFC и QR-коды. Bluetooth обеспечивает наибольшую универсальность и поддержку P2P-взаимодействия, QR-коды – доступность, а NFC – высокий уровень безопасности в ограниченных сценариях.

Использование данных технологий связано с необходимостью учета ключевых компромиссов: повышение приватности ограничивает контроль, автономность увеличивает риск двойного расходования, а усиление безопасности может снижать доступность системы.

Проведённый анализ позволяет сформулировать следующие рекомендации по реализации офлайн-транзакций в ЦВЦБ и представить схему выполнения офлайн-транзакции в ЦВЦБ.

Необходимо разделение онлайн- и офлайн-кошельков с предварительным переводом средств в офлайн-режим для локализации рисков.

Требуется локальная генерация и хранение криптографических ключей на устройстве пользователя.

Для защиты ключей и осуществления криптографических операций следует использовать Trusted Execution Environment (TEE).

Лимиты (по сумме, времени и параметрам транзакций) должны быть защищены от несанкционированного изменения.

Bluetooth целесообразно использовать как базовую технологию передачи данных, дополняя её другими решениями при необходимости.

Для офлайн-кошелька должны устанавливаться ограничения, включая лимиты на сумму, длину цепочки офлайн-транзакций и временные параметры использования.

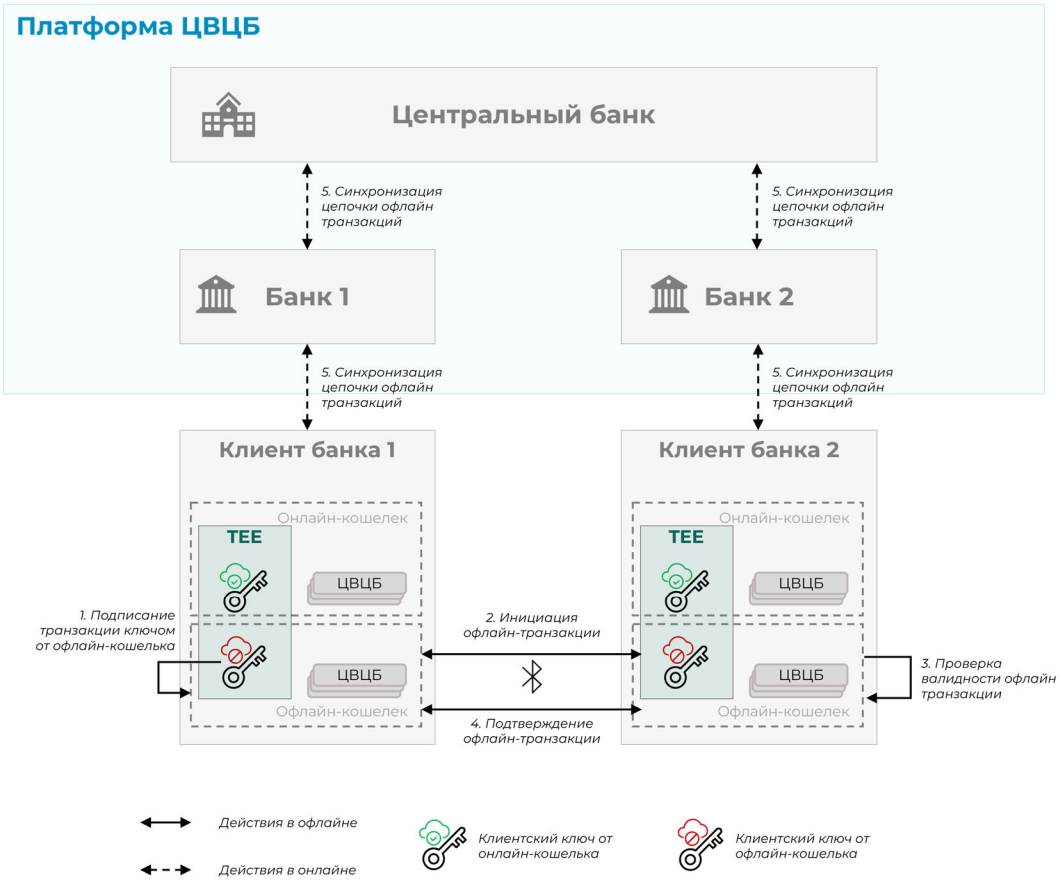

Рисунок 1. Архитектура выполнения офлайн-транзакции в ЦВЦБ (рисунок разработан автором в PowerPoint)

Таким образом, эффективная реализация офлайн-транзакций в ЦВЦБ требует сочетания архитектурного разделения средств, локальной криптографической защиты, системы лимитов и обоснованного выбора технологий передачи данных. Именно совокупность этих мер позволяет обеспечить баланс между доступностью, безопасностью и контролируемостью системы.

Список литературы:

1. Bank for International Settlements. Project Polaris: A handbook for offline payments with CBDC. – 2023. – ISBN 978-92-9259-652-1
2. John Kiff, Jihad Alwazir, Sonja Davidovic, Aquiles Farias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, Hunter K Monroe, Nobu Sugimoto, Hervé Tourpe, and Peter Zhou. A Survey of Research on Retail Central Bank Digital Currency // IMF Working Papers 2020. 104 (2020). DOI 10.5089/9781513547787.001
3. Bank for International Settlements. Project Polaris: A security and resilience framework for CBDC systems– 2023. – ISBN 978-92-9259-654-5
4. Bank for International Settlements. Project Polaris: A high-level design guide for offline payment – 2023. ISBN 978-92-9259-701-6
5. Bluetooth SIG. Bluetooth Core Specification. Part C. Generic Access Profile [Электронный ресурс]. – URL: https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host/generic-access-profile.html (дата обращения: 06.04.2026).
6. ГОСТ Р ИСО/МЭК 18004-2015. Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики

штрихового кода QR Code: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 3 июня 2015 г. N° 544-ст: дата введения 2016-02-01. – URL: https://docs.cntd.ru/document/1200121043 (дата обращения: 02.04.2026).

References:

1. Bank for International Settlements. Project Polaris: A handbook for offline payments with CBDC. – 2023. – ISBN 978-92-9259-652-1
2. John Kiff, Jihad Alwazir, Sonja Davidovic, Aquiles Farias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, Hunter K Monroe, Nobu Sugimoto, Hervé Tourpe, and Peter Zhou. A Survey of Research on Retail Central Bank Digital Currency // IMF Working Papers 2020, 104 (2020), DOI 10.5089/9781513547787.001
3. Bank for International Settlements. Project Polaris: A security and resilience framework for CBDC systems– 2023. – ISBN 978-92-9259-654-5
4. Bank for International Settlements. Project Polaris: A high-level design guide for offline payment – 2023. ISBN 978-92-9259-701-6
5. Bluetooth SIG. Bluetooth Core Specification. Part C. Generic Access Profile [Electronic resource]. – URL: https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host/generic-access-profile.html (date of access: 06.04.2026).
6. GOST R ISO/IEC 18004-2015. Information technology. Automatic identification and data capture techniques. QR Code barcode symbology specification: approved and enacted by Order of the Federal Agency for Technical Regulation and Metrology dated June 3, 2015 No. 544-st: effective date 2016-02-01. – URL: https://docs.cntd.ru/document/1200121043 (date of access: 02.04.2026).