

УДК 336.74

РАЗРАБОТКА МЕХАНИЗМОВ ВЗАИМОДЕЙСТВИЯ ОНЛАЙН КО-ШЕЛЬКА И ОФЛАЙН ПЛАТЕЖНЫХ ИНСТРУМЕНТОВ В РАМКАХ РАЗВИТИЯ ОФЛАЙН-ТРАНЗАКЦИЙ ЦБР

Ганчарова Д. Ю.¹, студент гр. 1д2101УИР, IV курс, Старовойтова Т. Ф.², к.э.н.,
доцент, доцент кафедры управления информационными ресурсами
Научный руководитель: Старовойтова Т. Ф.², к.э.н., доцент, доцент кафедры
управления информационными ресурсами

¹ Академия управления при Президенте Республики Беларусь, г. Минск,
Республика Беларусь

² Академия управления при Президенте Республики Беларусь, г. Минск,
Республика Беларусь

Стремительное развитие цифровых технологий в финансовом секторе и появление инновационных методов предоставления финансовых услуг, вопросы обеспечения безопасности, скорости и прозрачности транзакций становятся важнейшими задачами для финансовых регуляторов. Цифровая трансформация меняет экономическую активность и приводит к сокращению роли наличных денег, что, в свою очередь, стимулирует создание новых форм цифровых денег и существенно меняет ситуацию на уровне международных финансов [1].

Одним из наиболее значимых шагов в этом процессе стало внедрение криптовалют и технологий блокчейна, что привлекло внимание к концепции безналичного общества и цифровых валют. В ответ на эти изменения была выдвинута идея создания суверенных цифровых валют, или цифровых валют центральных банков (ЦВЦБ, англ. CBDC), представляющих собой цифровую форму национальной фиатной валюты, выпускаемой государством и являющейся законным платежным средством. Важно отметить, что стоимость ЦВЦБ эквивалентна стоимости национальной валюты в соотношении 1:1 [2].

В условиях быстрого внедрения цифровых валют и расширяющихся возможностей для проведения безналичных операций, одной из главных задач становится не только обеспечение доступности цифровых платежей, но и создание механизмов, которые позволяют проводить безопасные транзакции в условиях ограниченного доступа к сети. В данном контексте, развитие системы цифрового белорусского рубля (ЦБР) требует внедрения решений, которые обеспечат возможность безопасных офлайн-транзакций. Эти решения помогут преодолеть ограничения, связанные с необходимостью постоянного подключения к интернету, и откроют новые перспективы для пользователей, особенно в удалённых и труднодоступных регионах. Разработка таких технологий становится неотъемлемой частью стратегического развития ЦБР и ориентирована на

улучшение финансовой инклюзивности и безопасности транзакций в рамках новой цифровой экономики.

Таким образом, возникает необходимость в проработке и внедрении технологий для офлайн-операций, что подтверждается концепцией ЦБР. Согласно концепции: «использование офлайн-режима планируется реализовать в рамках дальнейшего развития ЦБР в связи с необходимостью проработки технологических и правовых аспектов, а также аспектов информационной безопасности.» [2].

Ранее в исследованиях предлагалась технология теневого кошелька, как одного из решений для защиты транзакций в офлайн-режиме [3]. В данной статье будут рассмотрены технологии взаимодействия теневого, офлайн и онлайн-кошельков в рамках системы ЦБР с целью повышения безопасности и удобства совершения транзакций в условиях ограниченного доступа к сети. Для обеспечения безопасности офлайн-платежей в системе ЦБР используется управление балансами и транзакциями через карты Stored Value Card.

Stored Value Card (SVC) или наличная карта – носитель, на котором хранится специальным образом зашифрованная стоимость, — деньги, минуты, литры, количество поездок, и т. д. [4].

Это означает, что платежным терминалам не требуется доступ к сети, так как средства можно снимать и вносить прямо с карты. Подобно наличным деньгам, такие карты могут быть использованы анонимно, владельцем карты. Данные карты представляют собой электронные эквиваленты токенов и находят применение в платёжных системах с низкой стоимостью или в случаях, когда доступ к сети затруднён или экономически нецелесообразен, например: в парковочных автоматах, системах общественного транспорта и закрытых платёжных системах, таких как на судах.

Решение опирается на надежную защиту систем посредников (в системе ЦБР – финансовые организации) и карт, а также на правильное управление системами администраторов, под администратором в рамках системы ЦБР рассматривается Национальный Банк Республики Беларусь.

Предполагается, что PoS-терминалы и мобильные устройства для офлайн-платежей могут быть уязвимы и подвержены атакам. Для обеспечения доверия между платежными инструментами и посредниками применяются цифровые сертификаты. В решении планируется использование самоподписанных сертификатов, однако для повышения безопасности в реальной системе рекомендуется также протестировать инфраструктуру открытого ключа (PKI) для выпуска, подписания и шифрования данных [5].

Кроме того, для синхронизации транзакций и предотвращения повторного использования одной и той же транзакции, должны быть реализованы счетчики и защита от атак с повторным воспроизведением. Каждая транзакция будет иметь уникальный идентификатор, который сохраняется в системах посредников, что обеспечивает защиту от мошенничества и повышает безопасность офлайн-платежей.

Механизмы взаимодействия онлайн кошелька и офлайн платежных инструментов в рамках развития офлайн-транзакций ЦБР.

При получении карты для офлайн платежей она не содержит средств. Для использования карты в офлайн-режиме пользователю необходимо предварительно перевести деньги с онлайн кошелька на карту. Предположительное решение по пополнению платёжных карт, приведено на рисунке 1, и предлагается осуществить следующим образом:

1. Пользователь открывает мобильное приложение финансовой организации (посредника), которая предоставляет доступ к платформе ЦРБ, и вводит сумму для перевода.
2. Для подтверждения операции пользователь вводит PIN-код в приложении и подносит карту к NFC-считывателю мобильного устройства.
3. Мобильное устройство генерирует запрос с цифровой подписью и отправляет его на узел посредника.
4. Посредник проверяет цифровую подпись и осуществляет перевод средств с онлайн-кошелька пользователя на теневой кошелёк.
5. После обновления баланса на теневом кошельке посредник подписывает новый баланс и передаёт его обратно в приложение.
6. Пользователь снова подносит карту к NFC-считывателю, и приложение обновляет баланс карты, передавая на неё подписанный баланс.
7. Баланс карты изменяется в соответствии с обновлённым значением, отражающим переведённые средства.

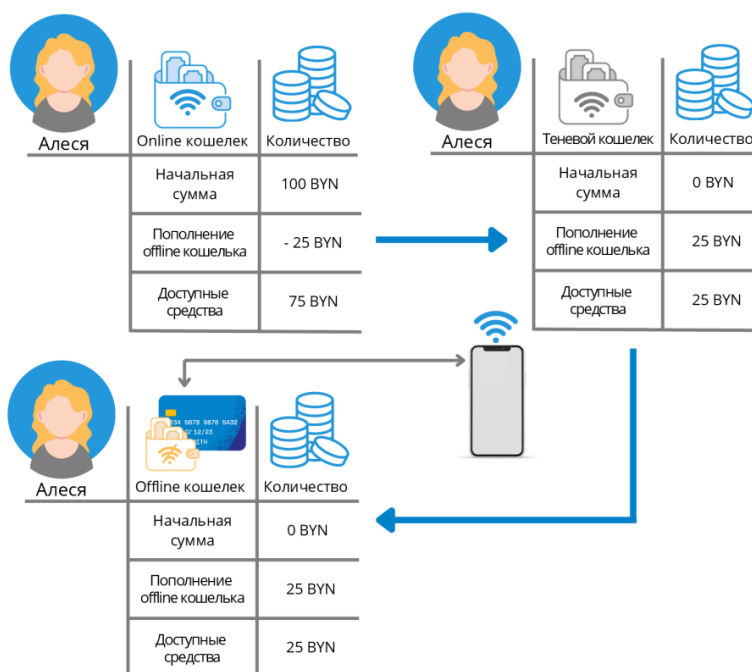


Рисунок 1. Процесс перевода средств с онлайн кошелька на офлайн кошелек

Примечание – собственная разработка.

Пользователь также может опустошить карту на любую сумму, процесс отображен на рисунке 2. Перед опустошением карты все офлайн-транзакции должны быть синхронизированы.

1. Пользователь открывает мобильное приложение финансовой организации, предоставляющее доступ к платформе ЦРБ, и вводит сумму, которую он желает вернуть.

2. Для подтверждения операции пользователь вводит PIN-код карты в приложении и подносит карту к NFC-считывателю мобильного устройства.

3. Карта проверяет введенный PIN-код и генерирует одноразовый код, который передаётся в приложение.

4. Приложение отправляет запрос посреднику на возврат средств, при этом посредник проверяет, что требуемая сумма доступна на теневом кошельке пользователя.

5. Посредник рассчитывает новый баланс теневого кошелька после уменьшения суммы и отправляет это значение с цифровой подписью обратно в приложение.

6. Пользователь снова подносит карту к NFC-считывателю мобильного устройства, и приложение передаёт подписанный баланс на карту.

7. Карта проверяет цифровую подпись и обновляет баланс.

8. Карта отправляет подтверждение о выполнении операции обратно в приложение, подписанное своей цифровой подписью.

9. Приложение передаёт это подтверждение посреднику.

10. Посредник проверяет подпись карты и завершает процесс перевода средств, переводя сумму с теневого кошелька пользователя на онлайн-кошелёк.

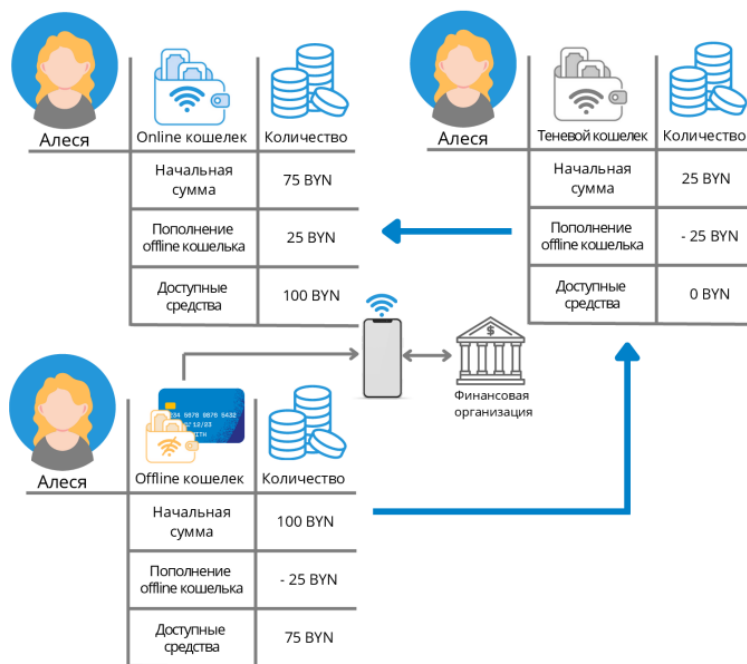


Рисунок 2. Процесс опустошения средств с офлайн кошелька
 Примечание – собственная разработка.

В результате предложенной схемы перевода средств между онлайн и офлайн кошельками можно сделать вывод, что данный процесс, хотя и обеспечивает функциональность офлайн-платежей, имеет ряд значительных недостатков. Во-первых, использование NFC-считывателей, PIN-кодов и цифровых подписей требует наличия нескольких технических компонентов и взаимодействия с посредниками, что увеличивает сложность и потенциальные точки отказа системы. Во-вторых, постоянная синхронизация данных между онлайн- и офлайн-системами требует значительных затрат на инфраструктуру, включая безопасность, хранение данных и поддержку криптографических механизмов.

Следует подчеркнуть, что предложенный процесс может быть неудобным для пользователей, особенно для тех, кто не обладает опытом работы с подобными технологиями. Это может привести к их сопротивлению внедрению новых методов оплаты и к стремлению избегать использования таких систем. Отсутствие привычки к выполнению таких операций, а также необходимость в дополнительном обучении потенциальных клиентов представляют собой значительные барьеры, которые могут затруднить массовое принятие и интеграцию этих технологий в повседневную финансовую практику.

Таким образом, для эффективного внедрения офлайн-платежей в систему цифрового рубля необходимо провести детальное исследование всех аспектов, включая технологические, финансовые и операционные затраты. Оценка возможных рисков и стоимости реализации позволит определить, оправданы ли такие вложения для системы ЦБР и соответствует ли это долгосрочной стратегии цифровой валюты, а также учесть возможные барьеры на пути адаптации пользователей.

Список литературы:

1. Головенчик, Г. Сравнительный анализ концепций цифровых валют Народного банка Китая и Банка России, оценка их применимости в Республике Беларусь [Текст] / Г. Головенчик, Гречко В. // Банковский вестник. – 2023. – № 2-715. – С. 52 – 63.
2. Концепция белорусского цифрового рубля [Электронный ресурс] // Национальный банк Республики Беларусь, 2025. – Режим доступа: https://www.nbrb.by/payment/digital_ruble/concept.pdf. – Дата обращения: 14.02.2025.
3. Ганчарова, Д. Ю. Интеграция технологии теневого кошелька в систему цифрового белорусского рубля [Текст] / Д. Ю. Ганчарова, И. В. Гваева // XXIX Международная научно-практическая конференция студентов и магистрантов «Теоретико-методологические и прикладные аспекты государственного управления». – Минск, 2024. – [в печати].
4. Карта предоплаты [Электронный ресурс] // Википедия – Режим доступа: https://web.archive.org/web/20151119173221/https://ru.wikipedia.org/wiki/Карта_предоплаты. – Дата обращения: 22.02.2025.
5. E-krona pilot Phase 4 [Электронный ресурс] // Riksbank, 2025. – Режим доступа: <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2024/e-krona-pilot-phase-4.pdf>. – Дата обращения: 23.02.2025.