МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра математической кибернетики и компьютерных наук

# АРХИТЕКТУРА ПРОГРАММНОГО ПРОДУКТА, ВЫПОЛНЯЮЩЕГО КРИПТОВАЛЮТНЫЕ ОПЕРАЦИИ С РАЗЛИЧНЫМИ ДЕЦЕНТРАЛИЗОВАННЫМИ КРИПТО-БИРЖАМИ НА БАЗЕ БЛОКЧЕЙНА ZKSYNC, И ВНЕДРЕНИЕ ДАННОГО ФУНКЦИОНАЛА В ПРИЛОЖЕНИЕ ДЛЯ УПРАВЛЕНИЯ КРИПТОВАЛЮТНЫМИ СЧЕТАМИ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 451 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Денисова Алексея Алексеевича

Научный руководитель
док. физ.-мат. наук, профессор _____ В. А. Романов

Зав.кафедрой
канд. физ.-мат. наук, доцент _____ С. В. Миронов

Саратов 2024

**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

После того, как Сатоши Накамото сделал революционную работу в 2008 году, опубликовав белую книгу «Bitcoin», появилось такое понятие, как децентрализованная валюта. Децентрализованная валюта — это цифровая валюта, не имеющая централизованного контроля, использующая децентрализованную сеть для записи и верификации транзакций. Сейчас децентрализованные валюты являются частью мировой экономики. По состоянию на 24 мая 2024 года под управлением биржевых биткоин-фондов хранится более 1 млн биткоинов на сумму около 69,1 млрд долларов, из которых более 70% были приобретены в 2024 году.

С развитием данных технологий появились инструменты и решения для взаимодействия с блокчейном и децентрализованными валютами. Блокчейн, как основа децентрализованных валют, предоставляет возможности для разработки и внедрения различных приложений. Приложение, или децентрализованная биржа (DEX), — это платформа для проведения различных финансовых операций без централизованного посредника. Биржа представляет собой инструменты для частично автоматической или полностью ручной торговли активами через непрямое взаимодействие с блокчейном. Подобные платформы для взаимодействия с децентрализованными валютами, в дальнейшем называемыми криптовалютами, имеют ряд недостатков:

1. Возможные атаки на биржи, ставящие под угрозу средства пользователей.
2. Сбои в работе системы, приводящие к замедлению или даже полной недоступности платформы, при росте числа активных пользователей.
3. Работа ботов, которые программно могут отправлять транзакции быстрее обычных пользователей, создавая неравные условия.
4. Низкая скорость обработки транзакций, что может привести к длительному ожиданию подтверждения операций.
5. Ограниченные возможности для работы с несколькими криптовалютными счетами одновременно.

Многие крупные организации и ведущие участники рынка отказываются от сотрудничества с биржами из-за перечисленных недостатков. Это указывает на необходимость разработки эффективного, удобного и надежного решения для осуществления криптовалютных операций.

Целью дипломной работы является разработка архитектуры программного продукта, выполняющего криптовалютные операции с различными децентрализованными крипто-биржами на базе блокчейна ZkSync, и внедрение данного функционала в приложение для управления криптовалютными счетами.

Таким образом, в рамках данной работы были поставлены следующие задачи:

1. Изучить архитектуру блокчейна ZkSync.
2. Изучить методы взаимодействия с децентрализованными крипто-биржами.
3. Реализовать модули, обеспечивающие взаимодействие с децентрализованными крипто-биржами.
4. Интегрировать разработанные модули в приложение для управления криптовалютными счетами.

## 1 Децентрализованная сеть ZkSync

ZkSync — это один из самых современных и технологичных масштабируемых решений для Ethereum, основанных на технологии Zk-Rollup. Блокчейн ZkSync обеспечивает высокую пропускную способность, низкие комиссии и мгновенное подтверждение транзакций. Он предназначен для решения проблем масштабируемости и высоких транзакционных издержек, присущих блокчейну Ethereum, сохраняя при этом высокий уровень безопасности и совместимость с существующими смарт-контрактами и децентрализованными приложениями. ZkSync широко популярен как среди пользователей (с более чем 5 миллионами активных участников), так и среди разработчиков. В сети ZkSync развернуто свыше 100 децентрализованных приложений.

**Децентрализованное приложение** — это платформа, работающая на основе блокчейна, которая предоставляет пользователям широкий спектр финансовых услуг, включая обмен цифровых активов, стейкинг, фермерство ликвидности, кредитование, заимствование, торговлю деривативами и NFT. В отличие от централизованных бирж (CEX), где все операции контролируются единой организацией, децентрализованные биржи функционируют по принципу децентрализованных финансов (DeFi), обеспечивая пользователям полный контроль над своими средствами и транзакциями. На DEX пользователи взаимодействуют напрямую через смарт-контракты, что повышает уровень безопасности, прозрачности и устойчивости к цензуре. Взаимодействие с децентрализованной биржей происходит через криптовалютный кошелек.

**Криптовалютный кошелек** — это программное или аппаратное средство для взаимодействия с сетью, это интерфейс для взаимодействия с блокчейном. Основная функция кошелька заключается в обеспечении безопасного способа выполнения транзакций, управления адресами и взаимодействия с децентрализованными приложениями (dApps) и блокчейном в целом.

Для выполнения самой популярной криптовалютной операции — обмена через интерфейс кошелька и децентрализованной биржи `KOI` в блокчейне ZkSync, пользователю нужно выполнить следующие действия:

1. Зайти на сайт приложения KOI (рисунок 1.1):

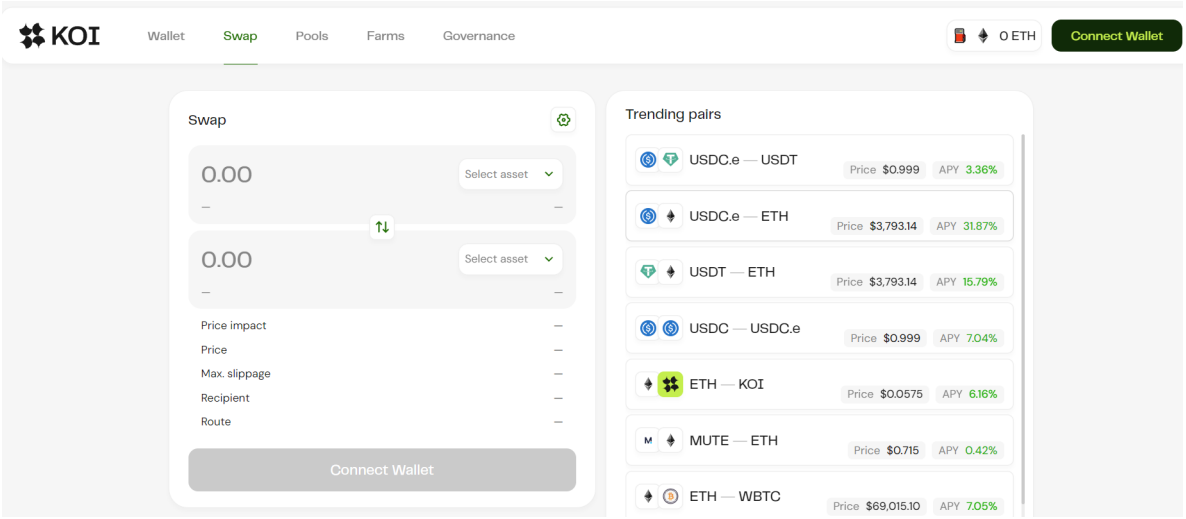


Рисунок 1.1 – Сайт децентрализованной биржи KOI

2. Подключить кошелек к бирже (рисунок 1.2):

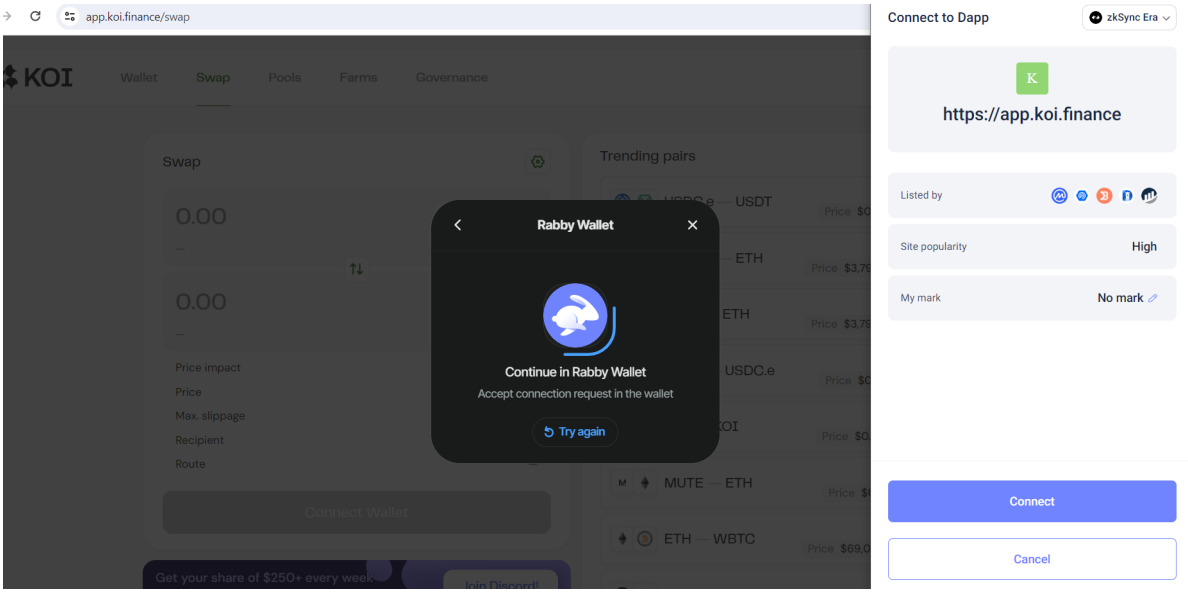


Рисунок 1.2 – Подключение кошелька к бирже

3. Ввести необходимый объем транзакции для обмена (рисунок 1.3):

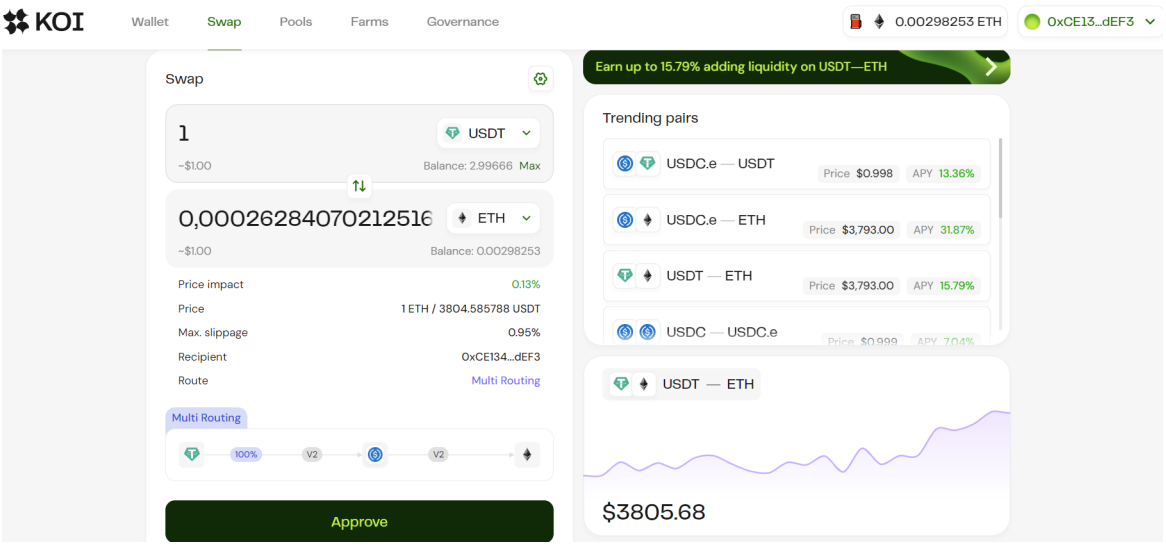


Рисунок 1.3 – Ввод объема транзакции для обмена

4. Подтвердить транзакцию в отдельно окне (рисунок 1.4):

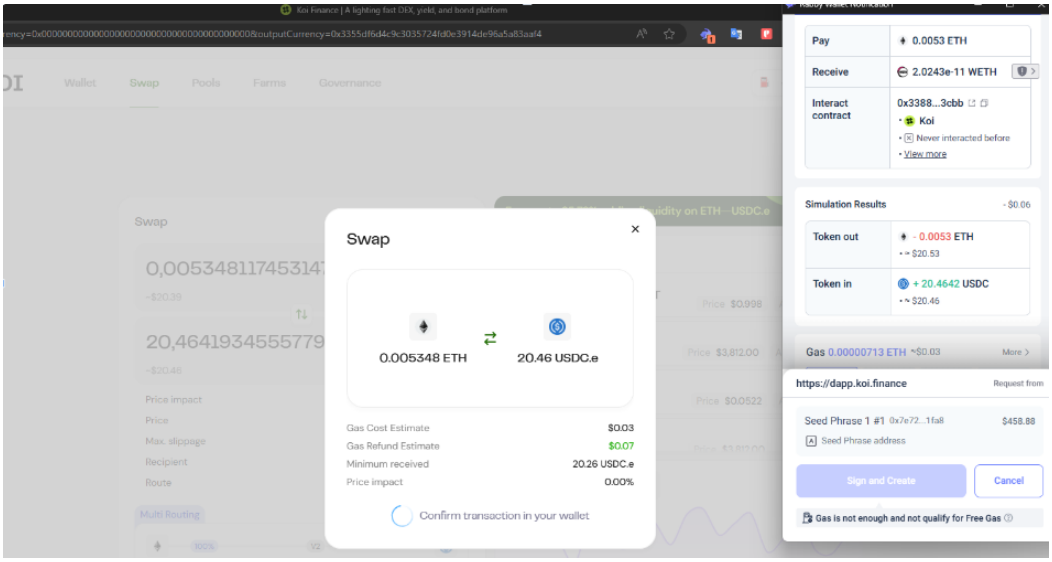


Рисунок 1.4 – Подтверждение транзакции

Архитектура взаимодействия пользователя с блокчейном ZkSync через интерфейс кошелька и децентрализованного приложения выглядит следующим образом (рисунок 1.5):

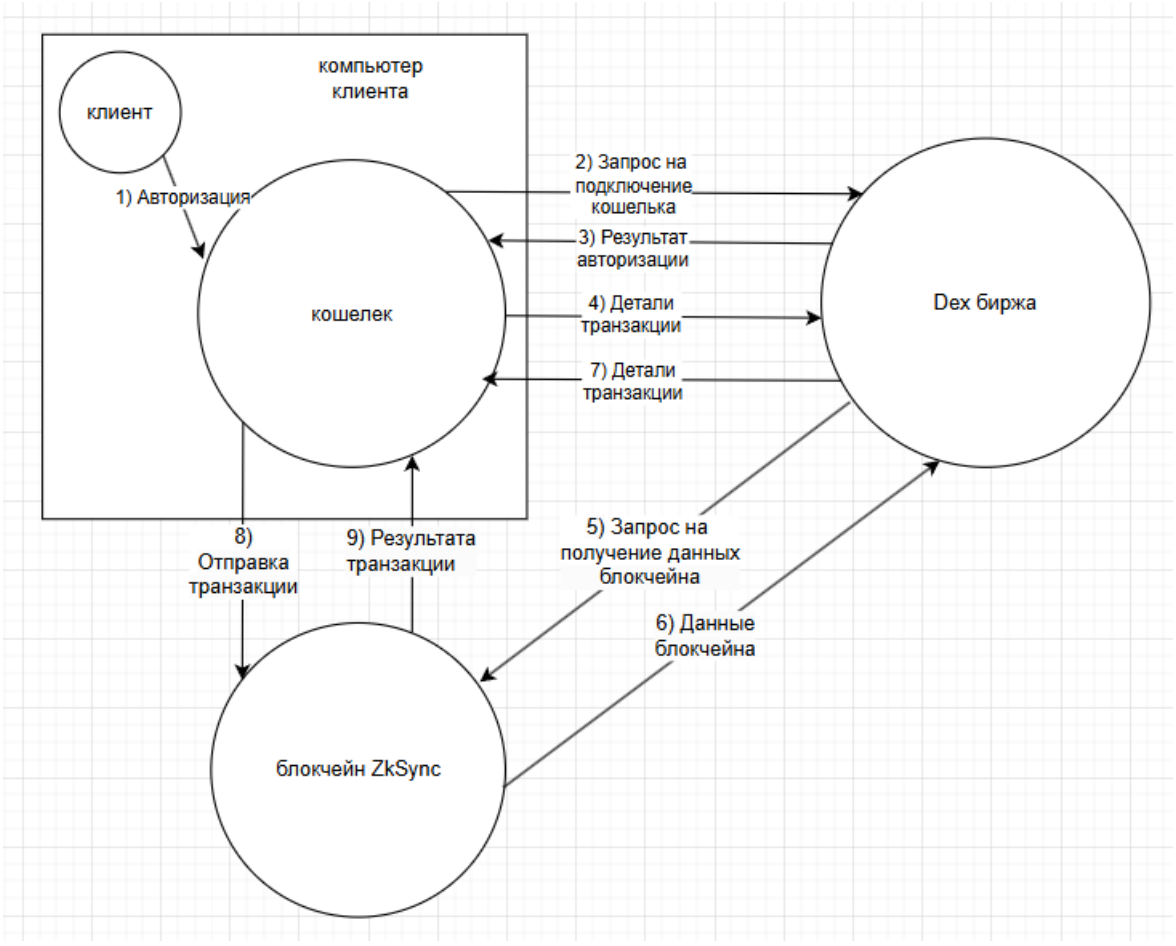


Рисунок 1.5 – Архитектура взаимодействия пользователя с блокчейном через интерфейс кошелька и децентрализованного приложения (номер означает порядок совершения операций)

Рассмотрим подробнее, что происходит на каждом этапе:

1. Авторизация пользователем с помощью мнемонической фразы или приватного ключа в криптовалютном кошельке, локально работающем на компьютере пользователя.
2. Отправка запроса на подключение кошелька к сайту биржи.
3. Получение кошельком запроса о результате авторизации.
4. Отправка деталей транзакции на сайт децентрализованного приложения
   - fromCcy: USDT
   - toCcy: ETH
   - amountFromCcy: 10

5. Получение биржей деталей транзакции и отправка запроса для получения дополнительных данных в блокчейн
   - nonce: 1
   - gas: 40000
   - gasLimit: 210000
   - amountToCcy: 0.003
6. Формирование полной транзакции со всеми необходимыми полями на основе полученных из блокчейна данных.
7. Отправка полной транзакции со всеми необходимыми полями кошельку.
8. Отправка транзакции в блокчейн для дальнейшего подтверждения.
9. Валидация транзакции в блокчейне и отправка результата выполнения транзакции пользователю.

Анализ представленной архитектуры показывает, что пользователь при совершении транзакции несколько раз взаимодействует с децентрализованной биржей, которая, в свою очередь, запрашивает данные из блокчейна. Это вызывает сомнения в целесообразности взаимодействия с биржей и поднимает вопрос о возможности прямого взаимодействия пользователя с блокчейном. Такой подход может устранить потенциальные ограничения, связанные с использованием посреднической биржи, которая имеет ряд недостатков:

1. Возможные атаки на биржи, ставящие под угрозу средства пользователей.
2. Сбои в работе системы, приводящие к замедлению или даже полной недоступности платформы, при росте числа активных пользователей.
3. Работа ботов, которые программно могут отправлять транзакции быстрее обычных пользователей, создавая неравные условия.
4. Низкая скорость обработки транзакций, что может привести к длительному ожиданию подтверждения операций.
5. Ограниченные возможности для работы с несколькими криптовалютными счетами одновременно.

Чтобы выполнять транзакции, взаимодействуя напрямую с блокчейном, нужно получить из сети необходимые для формирования транзакции данные (nonce, gas, gasLimit, amountToCcy), которые децентрализованное приложение получает из блокчейна. Фактически нужно создать приложение, которое будет

включать в себя функционал и криптовалютного кошелька, и биржи. Архитектура данного решения выглядит следующим образом (рисунок 1.6):

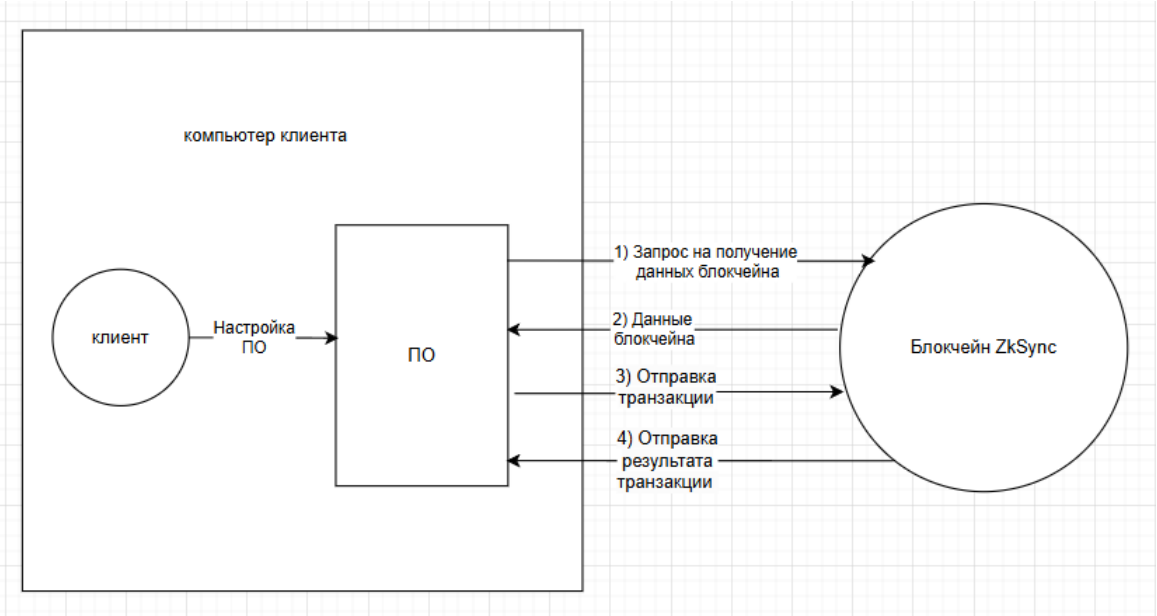


Рисунок 1.6 – Архитектура решения для прямого взаимодействия с блокчейном

Рассмотрим подробнее, что происходит на каждом этапе:

1. Запрос на получение необходимых данных из блокчейна:
   - nonce: 1
   - gas: 40000
   - gasLimit: 210000
   - amountToCcy: 0.003.
2. Получение необходимых данных и формирование транзакции.
3. Отправка транзакции в блокчейн для дальнейшего подтверждения.
4. Валидация транзакции в блокчейне и отправка результата выполнения транзакции пользователю.

Анализ представленной архитектуры показывает, что пользователь, взаимодействуя с блокчейном напрямую через локально установленное программное обеспечение, достигает того же результата (получение результата выполнения транзакции), что и при взаимодействии через интерфейс кошелька и децентрализованную биржу.

## 2 WEB3, как средство для взаимодействия с блокчейном

Web3py — это библиотека Python, которая позволяет разработчикам создавать децентрализованные приложения и взаимодействовать с блокчейн-сетями. Для реализации прямого взаимодействия пользователя с блокчейном без посредников, таких как децентрализованные биржи, можно использовать библиотеку Web3py. Основные возможности данной библиотеки включают в себя:

1. **Взаимодействие с блокчейном**. Web3py предоставляет функции для подключения к блокчейн-узлам, отправки транзакций и выполнения смарт-контрактов. Это позволяет разработчикам и пользователям взаимодействовать с блокчейном напрямую.
2. **Управление учетными записями**. Web3.py поддерживает создание и управление криптовалютными счетами, включая генерацию новых адресов и управление приватными ключами, что обеспечивает безопасность и контроль над средствами.
3. **Отправка и получение транзакций**. Web3.py упрощает процесс создания, подписания и отправки транзакций в блокчейн, обеспечивая их корректное исполнение и валидацию.
4. **Выполнение смарт-контрактов**. Библиотека позволяет развертывать и выполнять смарт-контракты, что открывает возможности для создания сложных децентрализованных приложений и автоматизации процессов.
5. **Подключение к различным провайдерам**. Web3.py поддерживает подключение к различным провайдерам блокчейн-инфраструктуры, таким как Infura, MetaMask и локальные узлы Ethereum, обеспечивая гибкость и надежность соединения.

Таким образом, библиотека Web3py поможет получить недостающие необходимые данные для формирования транзакции (nonce, gas, gasLimit, amountToCcy) и отправить её в сеть для дальнейшего подтверждения нодами блокчена ZkSync.

## 3 Новый подход для взаимодействия с блокчеком напрямую

Прежде чем описывать разработку всех модулей приложения для взаимодействия с сетью zkSync, необходимо описать архитектуру всего приложения.

Архитектура приложения выглядит следующим образом (рисунок 3.1):

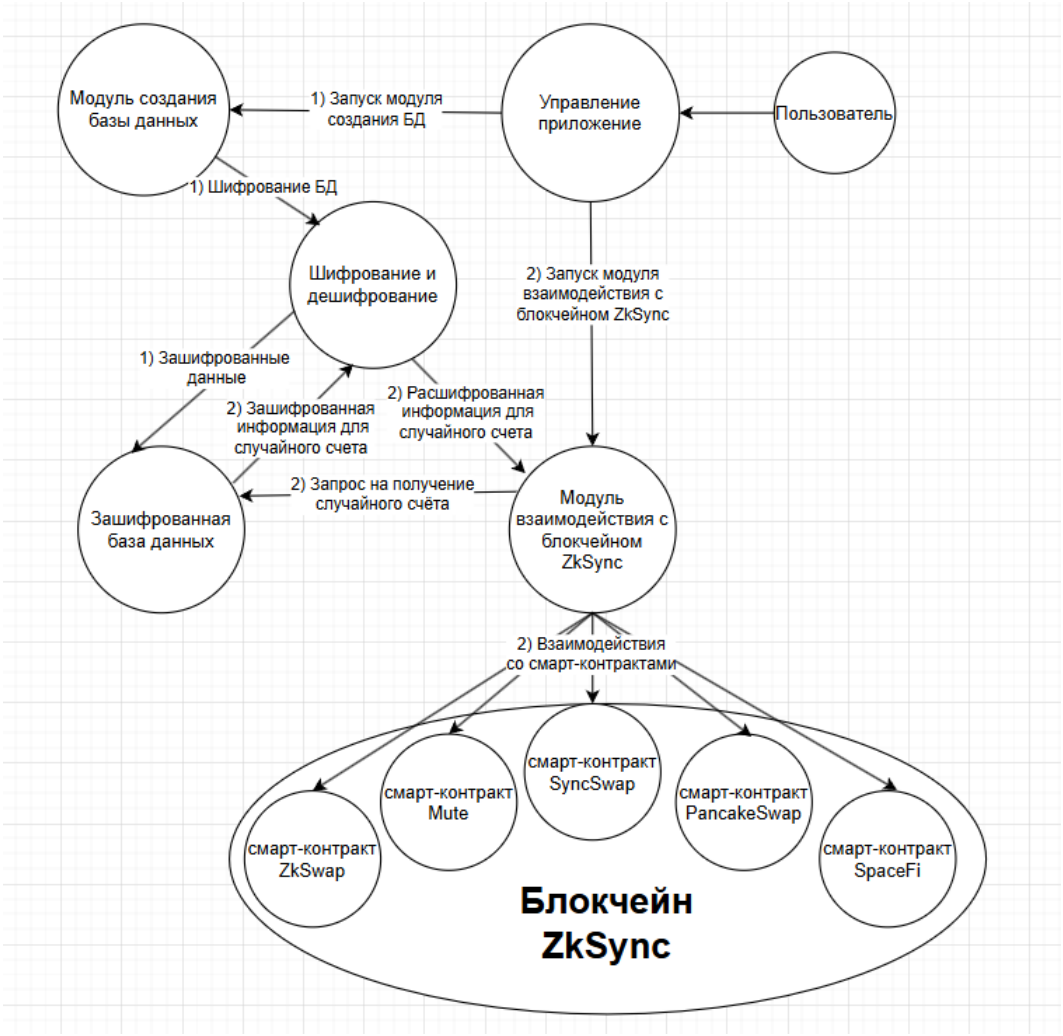


Рисунок 3.1 – Архитектура приложения (числами показывается различные сценарии взаимодействия, выбранные пользователем)

Пользователь, управляя приложением, может выбрать модуль создания базы данных или модуль взаимодействия с блокчейном. *Модуль создания базы данных* отвечает за хранение всех операций взаимодействия с блокчейном, обеспечивая возможность восстановления и продолжения работы с того же места даже после перезапуска приложения. *Модуль взаимодействия с блокчейном* считывает операции из базы данных и выполняет их. Важно отметить, что модуль взаимодействия с блокчейном требует наличия предварительно созданной базы данных для корректной работы.

Для наглядного представления поведения приложения, продемонстрируем диаграмму деятельности, показанную на рисунке 3.2.

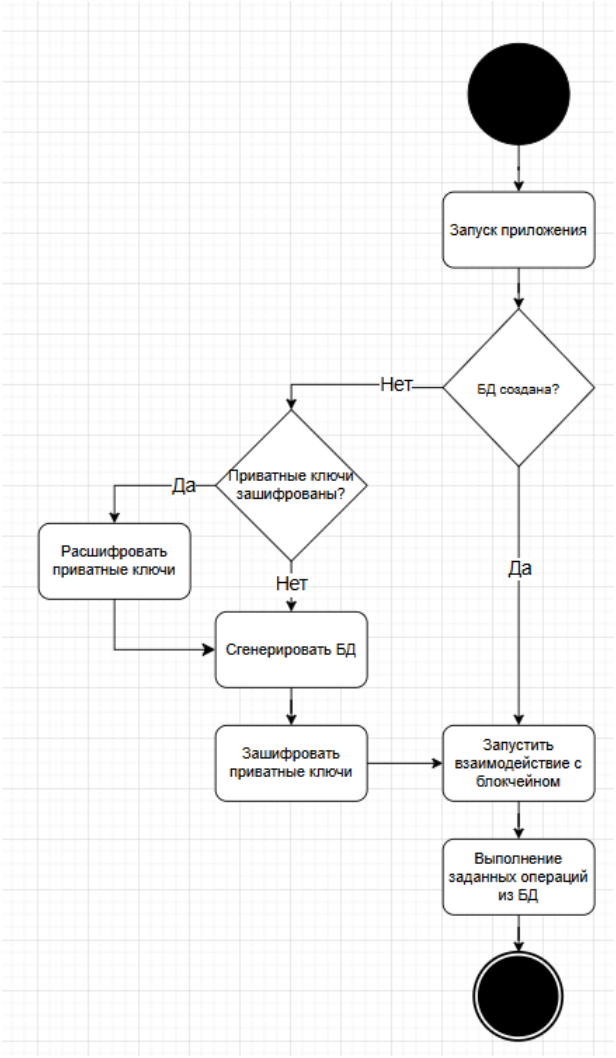


Рисунок 3.2 – Диаграмма деятельности приложения

Общая архитектура всего приложения показана на диаграмме классов ниже:

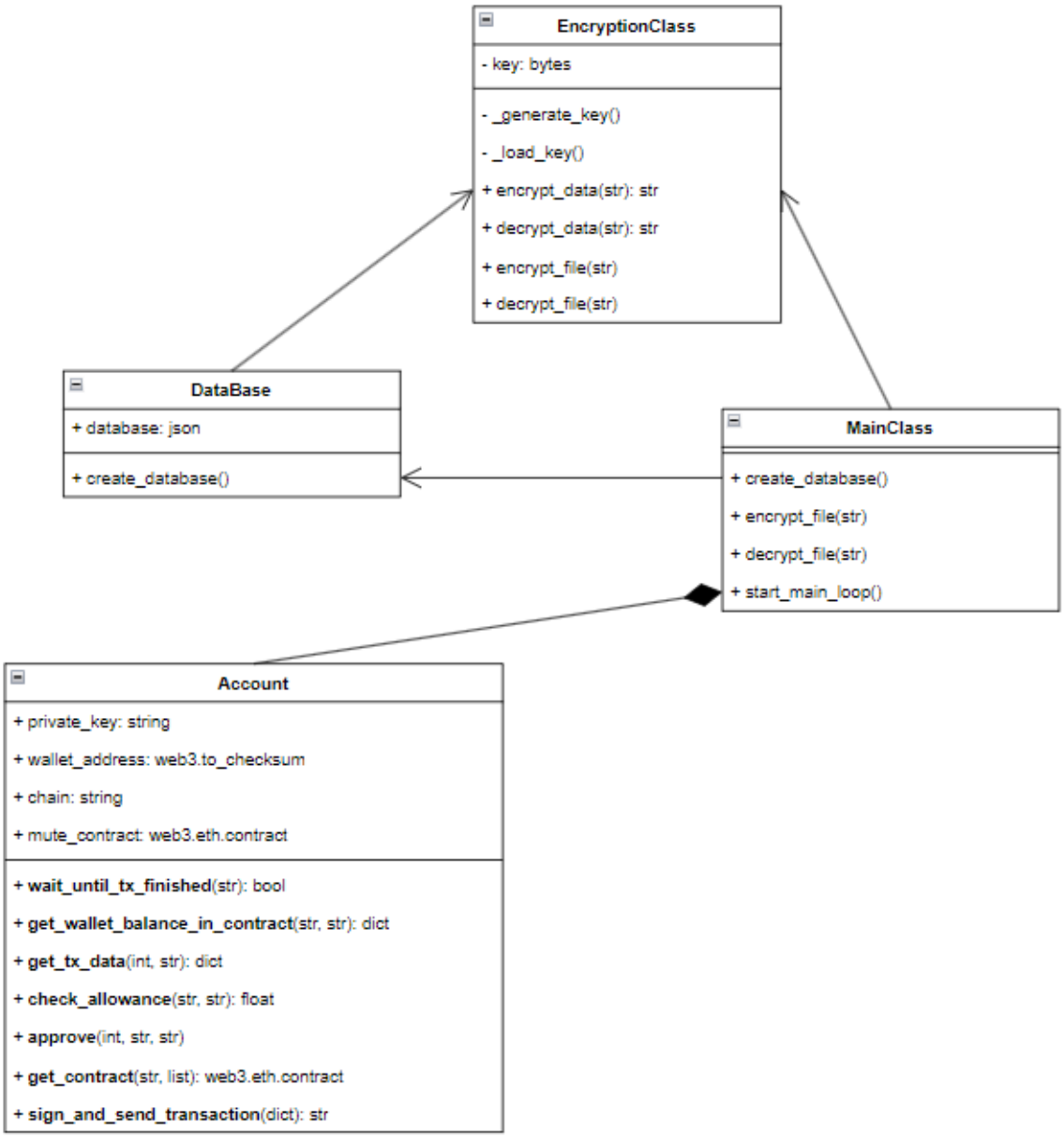


Рисунок 3.3 – Диаграмма классов приложения

Основной функционал приложения, включая взаимодействие с модулями, описывается следующим образом:

1. В файле main.py (этот файл реализует «модуль управления приложением» на диаграмме 3.1) пользователь имеет возможность выбирать одно из следующих действий:
   *а*) зашифровать файл с приватными ключами;
   *б*) расшифровать файл с приватными ключами;
   *в*) создать цикл работы с аккаунтами и применить модули взаимодействия с децентрализованными биржами ко всем аккаунтам из БД;

*г*) сгенерировать базу данных аккаунтов;

*д*) завершить работу приложения.

2. При выборе функции шифрования или расшифрования файла с приватными ключами происходит шифрование или дешифрование файла (модуль шифрования на диаграмме 3.1).
3. При выборе функции генерации БД (модуль базы данных), программа создает базу криптовалютных счетов по следующему алгоритму:

   *а*) считывается список приватных ключей криптовалютных кошельков;

   *б*) происходит итерация по каждому приватному ключу;

   *в*) извлекается из приватного ключа открытый ключ;

   *г*) шифруется закрытый ключ;

   *д*) формируется список необходимых модулей в виде двунаправленного взаимодействия (например, если есть токен A, он меняется на Mute бирже на токен B, а далее операция повторяется, но в обратную сторону) и полученный список перемешивается для достижения рандомизации между действиями счетов;

   *е*) запись вида

   ```
   publickey: {"pk": privatekey, "modules": shuffled_list_modules}
   ```

   добавляется в базу данных.
4. При выборе создания цикла работы с аккаунтами из БД, действия происходят по следующему алгоритму:

   *а*) считываются данные из БД;

   *б*) собирается из полученных данных приватный и публичный ключи, а также список применяемых модулей для каждого аккаунта, после чего приватный ключ проходит этап дешифрования;

   *в*) для каждой пары собранных приватных и публичных ключей создается объект аккаунта и добавляется в список;

   *г*) создается цикл работы с аккаунтами, который на каждой итерации случайным образом выбирает следующий аккаунт для обработки и выполняет все собранные из БД операции для него (все используемые в приложении модули показаны на диаграмме 3.1 как соединенные с классом Account);

   *д*) цикл работает до тех пор, пока все модули для каждого из аккаунтов не будут выполнены, после цикл работы приложения завершается.

## ЗАКЛЮЧЕНИЕ

Таким образом, в ходе последовательного решения всех поставленных задач, включающих:

1. Изучение архитектуры блокчейна ZkSync.
2. Изучение методов взаимодействия с децентрализованными крипто-биржами.
3. Реализация модулей, обеспечивающих взаимодействие с децентрализованными крипто-биржами.
4. Интеграция разработанных модулей в приложение для управления криптовалютными счетами.

была успешно дистигнута цель разработка архитектуры программного продукта, выполняющего криптовалютные операции с различными децентрализованными крипто-биржами на базе блокчейна ZkSync, и апробация данного функционала в приложение для управления криптовалютными счетами. Преимущества данного подхода включают в себя:

- взаимодействие с несколькими криптовалютными счетами одновременно;
- высокая скорость обработки транзакций;
- высокий уровень безопасности благодаря тому, что приложение работает локально на компьютере пользователя;
- защиту от ботов, поскольку объемы транзакций настраиваются заранее в приложении, исключая необходимость ручного ввода и ускоряя процесс отправки;
- решение проблемы, низкой пропускной способности в период пиковой нагрузки.

Разработанное приложение позволяет пользователям эффективно управлять своими криптоактивами, минимизируя риски, связанные с централизованными посредниками, и оптимизируя процесс взаимодействия с блокчейном. Интеграция с блокчейном ZkSync обеспечивает масштабируемость и низкие комиссии, что делает приложение удобным и экономически выгодным инструментом для всех категорий пользователей, от начинающих до опытных трейдеров. Внедрение таких решений способствует дальнейшему развитию децентрализованных финансов и поддержке использования криптовалют в экономике.