Проектирование и реализация среды исполнения смарт-контрактов для блокчейна Hyperledger Iroha

Иван Тюляндин
Научный руководитель: ст. преп. Я. А. Кириленко
Консультант: к. ф.-м. н. Д. А. Березун
Рецензент: ген. дир. “Сорамитсу Лабс” К. Р. Салахиев

11 июня 2019

Предметная область

Смарт-контракт

Программа, описывающая сделку участников блокчейн-сети. Запускается автоматически при достижении условий. Имеет преимущества перед бумажным контрактом.

Hyperledger Iroha

Open-source блокчейн консорциума Hyperledger (https://github.com/hyperledger/iroha).

Цель

Цель

Инфраструктура поддержки среды исполнения смарт-контрактов для блокчейна Hyperledger Iroha.

Смарт-контракты повысят доверие внутри сети и степень автоматизации договоров. Разработчики Hyperledger Iroha хотят попробовать различные среды исполнения смарт-контрактов.

Поставленные задачи

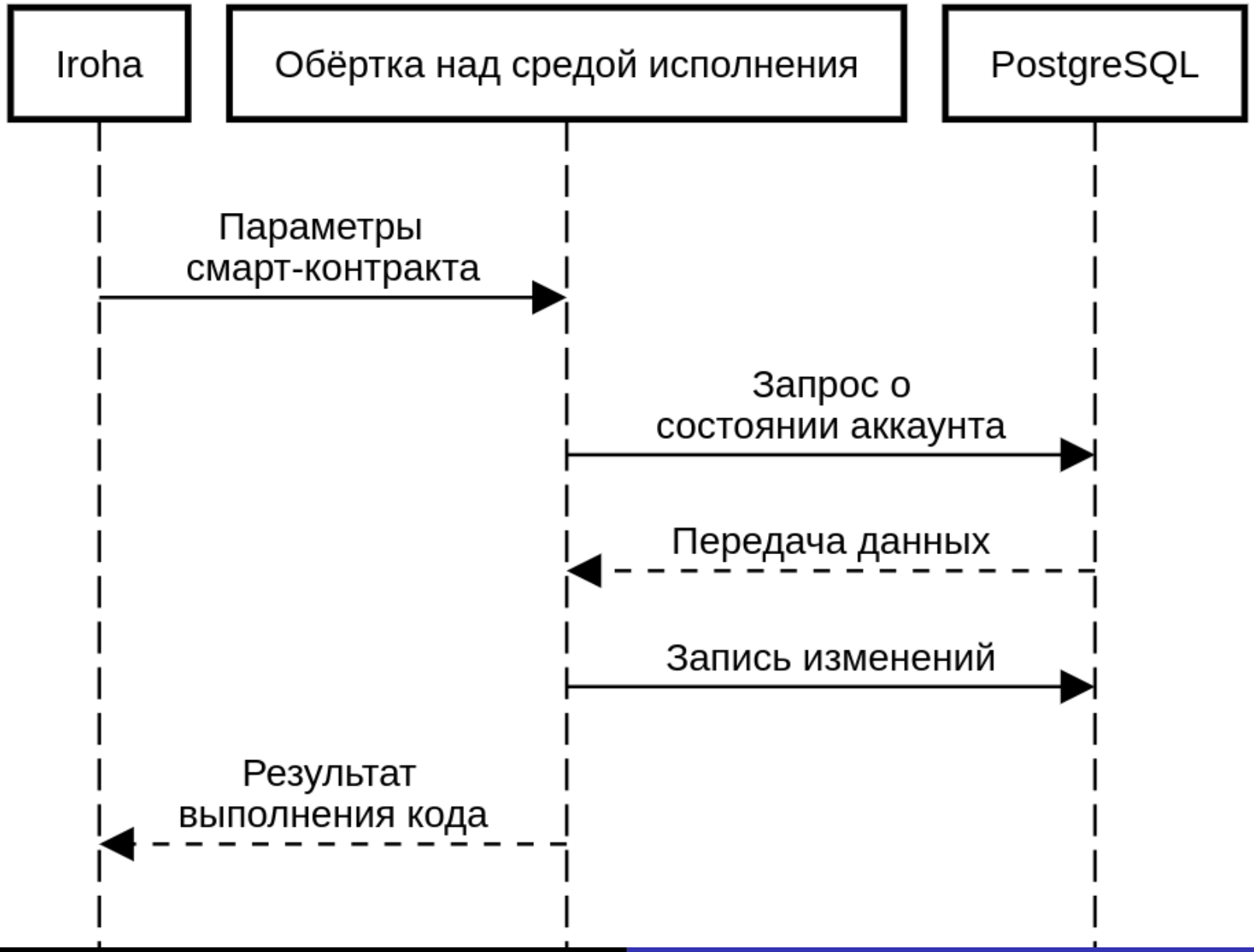
- Выполнить обзор существующих языков и сред исполнения смарт-контрактов
- Разработать архитектуру и программный интерфейс для взаимодействия среды исполнения смарт-контрактов с Hyperledger Iroha
- Реализовать взаимодействие одной из сред исполнения смарт-контрактов с Hyperledger Iroha
- Провести тестирование добавленной функциональности

Интерфейс взаимодействия

Транзакция формируется с помощью команд управления активами.

Добавлена новая команда для работы со средой исполнения смарт-контрактов. Основная задача — передать необходимые параметры.

Диаграмма выполнения смарт-контракта



Необходимая функциональность для интеграции

- Передача параметров внутри системы
- Чтение и запись актуального состояния через базу данных
- Формирование данных на входе и выходе среды исполнения смарт-контрактов

Обзор существующих сред исполнения и языков смарт-контрактов

Обзорная статья *A Survey of Smart Contract Safety and Programming Languages* принята к публикации в Трудах ИСП РАН.

Известные — Ethereum (Solidity, Viper), Bitcoin. Параметры сравнения: парадигма, Тьюринг-полнота, экосистема и другие.

Ethereum — одна из самых развитых платформ.

Среда исполнения

Hyperledger Burrow

Реализация блокчейна со смарт-контрактами из Ethereum (https://github.com/hyperledger/burrow).

Преимущества

- Интерфейс для работы с Ethereum Virtual Machine
- Поддерживается сообществом Hyperledger
- Есть примеры интегрирования (Hyperledger Fabric и Hyperledger Seth)

Недостатки

- Специфичная предметная область

Тестирование

Команда управления

- Валидация данных
- Операции по переводу в другой формат

Взаимодействие со средой исполнения

- Чтение
- Запись
- Вызов функций

Результаты

- Выполнен обзор существующих сред исполнения и языков смарт-контрактов, обзорная статья принята к публикации в сборнике трудов ИСП РАН
- Разработаны архитектура и программный интерфейс для взаимодействия среды исполнения смарт-контрактов с Hyperledger Iroha
- Реализовано взаимодействие Hyperledger Iroha и среды исполнения смарт-контрактов проекта Hyperledger Burrow
- Проведено модульное и интеграционное тестирование

Использованные технологии

Языки

C++, Go, Solidity

Библиотеки

Libpq, GTest, Boost, Protobuf, RapidJSON

Дополнительно

PostgreSQL, EVM, CMake, Git, Docker

Передача параметров

Взаимодействие C++ и Go

Использование флага компилятора Go для создания разделяемой библиотеки (shared object) и заголовочного файла на языке C из обёртки над виртуальной машиной из Hyperledger Burrow.