Федеральное агентство связи

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»

**Кафедра Математической кибернетики и информационных технологий**

Документация к практической работе

Платформа blockchain Waves, и язык скриптов RIDE

Выполнил студент

группы БВТ1702

Тимчук А.В.

Оглавление

[1 Обзор платформы Waves 3](#_Toc13302300)

[1.1 Введение 3](#_Toc13302301)

[1.2 Основополагающие принципы 3](#_Toc13302302)

[2 Язык скриптов RIDE 4](#_Toc13302303)

[2.1 Введение 4](#_Toc13302304)

[2.2 Типы скриптов 5](#_Toc13302305)

[2.3 Переменные 5](#_Toc13302306)

[2.4 Комментарии 5](#_Toc13302307)

[2.5 Типы данных 6](#_Toc13302308)

[2.6 Функции 7](#_Toc13302309)

[2.7 Исключения 7](#_Toc13302310)

[2.8 Исполнение 7](#_Toc13302311)

# 1 Обзор платформы Waves

## Введение

**Waves Platform** — открытая блокчейн платформа, разработанная для простоты использования и массового внедрения технологии блокчейн. Это комплексная блокчейн-экосистема, которая предоставляет все необходимые функции для внедрения технологии блокчейн в бизнес.

Платформа построена на базе модульного фреймворка Scorex, разработанного на языке Scala.

Платформа предоставляет возможность создания смарт-контрактов (контрактов со скриптами), которые включают в себя контроль над аккаунтом и над токенами, и предоставляют всё необходимое для реализации таких функций, как кошелёк с мультиподписью, atomic swap, двухфакторная аутентификация. Также Waves вводит новый тип транзакции - “Data Transaction”. Data Transaction - это способ публикации Oracle-данных в блокчейн при помощи смарт-контракта. Для создания скриптов для контрактов на этой платформе используется язык программирования RIDE.

## 1.2 Основополагающие принципы

Механизм подтверждения долей — в отличие от других блокчейн платформ в Waves подтверждением права работать в системе является доля, то есть многие функции сети доступны только при положительном балансе.

Нет генерации «из воздуха» — в отличие от других блокчейн платформ в Waves не происходит генерация токенов «из воздуха», при обслуживании транзакции снимается комиссия.

Шлюзы — механизмы, позволяющие вводить и выводить реальные средства. Пользователи Waves могут вносить депозиты в долларах США и евро через безопасные шлюзы, получая взамен токен, который на 100% обеспечивается резервами USD или EUR. Введённые средства могут храниться, передаваться и обмениваться на другие токены быстро и недорого, а также, могут быть выведены через шлюз обратно в традиционную финансовую систему.

Шлюзы USD и EUR предлагают пользователям Waves легкий способ перевести деньги в блокчейн систему, позволяя им инвестировать в токены и ICO с помощью фиата. Это одно из ключевых предложений платформы Waves: возможность отправлять и торговать с помощью физически-обеспеченных токенов.

Децентрализованная биржа — позволяет размещать и выполнять заявки на покупку или продажу криптовалюты или токенов за другую криптовалюту или обменивать их на другие токены (в т.ч. фиат).

# 2 Язык скриптов RIDE

## 2.1 Введение

**RIDE** — функциональный язык программирования, основанный на выражениях.

* + Имеет сильную статическую типизацию
  + Не имеет циклов, рекурсий и goto-подобных выражений, и поэтому является неполным по Тьюрингу
  + По замыслу ленивый
  + Появился в 2018 году.
  + Для разработки может использоваться Waves IDE или Visual Studio Code с расширением waves-ride.
  + Сложность скрипта на RIDE — безразмерная величина, которая оценивает вычислительные ресурсы необходимые для исполнения скрипта на RIDE, оценивается исходя из сложностей всех операторов и функций, составляющих скрипт.

## 2.2 Типы скриптов

dApp-скрипты — скрипт приложения, прикрепляется к аккаунту. Директивы: {-# CONTENT\_TYPE DAPP #-}.

Скрипты аккаунтов — обычный скрипт, прикреплённый к аккаунту. Директивы: {-# CONTENT\_TYPE EXPRESSION #-}, {-# SCRIPT\_TYPE ACCOUNT #-}.

Скрипты ассетов — обычный скрипт, прикреплённый к ассету. Директивы: {-# CONTENT\_TYPE EXPRESSION #-}, {-# SCRIPT\_TYPE ASSET #-}.

## 2.3 Переменные

В языке RIDE все переменные являются неизменяемыми (immutable variables). Это значит, что как только мы присвоили значение переменной, её значение в будущем уже нельзя будет изменить. Переменные в RIDE работают, как переменные-константы в основных языках программирования.

let — ключевое слово, с помощью которого неизменяемой переменной присваивается значение ленивым образом (слово let работает, как lazy val в языке Scala).

Значение переменной, определённой с помощью ключевого слова let, будет вычислено только в момент её первого использования.

## 2.4 Комментарии

Для написания комментариев в коде используется символ #. Все комментарии однострочные.

## 2.5 Типы данных

Базовые типы:

* 1. Boolean
  2. ByteVector
  3. Int
  4. String

Специальные типы:

* 1. List
  2. Nothing
  3. Unit

Предопределённые структуры:

* 1. Address — Структура адреса
  2. Asset — Структура токена
  3. AssetPair — Структура пары токенов ордера
  4. AttachedPayment — Структура платежа транзакции вызова скрипта
  5. BlockInfo — Структура блока
  6. DataEntry — Структура записи хранилища данных аккаунта
  7. Invocation — Структура сокращенного представления транзакции вызова скрипта
  8. Order — Структура ордера
  9. ScriptResult — Структура результата выполнения вызываемой функции
  10. ScriptTransfer — Структура перевода токенов
  11. Transfer — Структура перевода токенов транзакции массового перевода
  12. TransferSet — Структура списка переводов токенов
  13. WriteSet — Структура списка записей хранилища данных аккаунта

Создание пользовательских структур невозожно.

## 2.6 Функции

Функция должна возвращать значение.

В сигнатуре функции тип возвращаемого значения не указывается.

Функция должна быть объявлена выше места её использования.

Пример объявления функции:

func main(amount: Int, name: String) = {

5

}

Для возвращения результата не используется ключевое слово return, результат просто записывается в конце функции.

В языке определён небольшой набор встроенных функций.

## 2.7 Исключения

Исключения выбрасываются с помощью функции throw, которая имеет возвращаемый тип Nothing.

В RIDE нет обработки исключений. После того как исключение было выброшено, скрипт прекратит своё выполнение. Транзакция при этом будет считаться неудавшейся и не будет включена в блок.

## 2.8 Исполнение

Различные типы скриптов исполняются по разному.

Скрипты привязанные к аккаунтам используются, например, для верификации транзакций, то есть проверяют отправляемые транзакции на допустимость. Они исполняются каждый раз при совершении транзакции.

Скрипты приложений предоставляют набор функций, которые могут быть вызваны. Они исполняются при поступлении на аккаунт транзакции вызова функции.

Скрипты прикреплённые к ассетам (токенам) регулируют оборот токенов. Они вызываются при передаче токена в транзакции.