

Программа учебной дисциплины «Разработка смарт-контрактов и приложений для распределенных реестров»

Утверждена
Академическим советом ООП
Протокол № 2.03-09/2706-01 от «27» июня 2018г.

Автор	Суворова Ольга
Число кредитов	6
Контактная работа (час.)	40
Самостоятельная работа (час.)	188
Курс	2
Формат изучения дисциплины	full time

1 Цели освоения дисциплины

Целями освоения дисциплины [Введите название дисциплины из ОУП] являются получение знаний о технологии распределенного реестра и языках программирования для реализации блокчейн-проектов, развитие понимания связи теоретических основ с решением практических задач.

Для освоения учебной дисциплины студенты должны владеть следующими знаниями и компетенциями:

знать:

- Предпосылки и историю возникновения технологии блокчейн;
- Основы криптографии;
- Специфику работы блокчейн-платформ Bitcoin, Ethereum, Hyperledger;
- Примеры реализованных проектов.

уметь:

- Прописывать архитектуру блокчейн-проектов;
- Анализировать необходимые технические решения для реализации;
- Создавать смарт-контракты;
- Оценивать смарт-контракты других проектов;
- Ставить задачи для разработки блокчейн-проектов;
- Генерить идеи проектов с применением технологии.

владеть:

- Основными навыками для создания проектов с применением технологии блокчейн
- Языком программирования Solidity;
- Технологией создания проектов на платформе Ethereum;
- Спецификой создания проектов на платформе HyperLedger.

2 Формы контроля знаний студентов

Тип контроля	Форма контроля	2 год		Кафедра/подразделени е	Параметры **
		1	2		
Текущий	Контрольная работа	+	+		Тестирование не менее 20 вопросов
	Домашнее задание		+		Задача на программирование (не менее 2 акд. часов трудоемкость)
	Лабораторная работа		+		Задача на программирование (не менее 1 акд. часов трудоемкость)
	Проект				Устный опрос
	Другие формы (указать)				
Промежуточный	Экзамен				Презентация из 8 слайдов, устная защита
Итоговый	Экзамен				Разработка прототипа. Презентация из 8 слайдов, устная защита.

3 Критерии оценки знаний, навыков

№ п/п	Вид занятия	Форма проведения занятий	Цель
1	лекция	изложение теоретического материала	получение теоретических знаний по дисциплине
2	лекция	изложение теоретического материала с помощью презентаций	повышение степени понимания материала
3	решение лабораторных задач, семинары	решение задач по заданию преподавателя – решаются задачи, выданные преподавателем по итогам лекционных занятий, используются электронный конспект лекций и учебники, рекомендуемые данной программой	осознание связей между теорией и практикой, а также взаимозависимостей разных дисциплин
4	самостоятельная работа студента	2 домашних задания; прием работы происходит удаленно в виде ручного ревью кода	контроль уровня овладения практическим навыком решения задач.
5	контрольная работа	2 аудиторские работы в виде тестирования	контроль усвоения теоретического материала, а также уровень овладения практическим навыком решения задач.

4 Содержание дисциплины

№п/п	Тема (раздел) дисциплины
1	Вводный курс в технологию блокчейн и криптографию
1.1	Введение в технологию блокчейн: основные термины и понятия, принципы работы технологии, биткойн и альткойны, создание криптовалют, технический механизм работы криптовалют, транзакции в сети. Децентрализация и централизация. Распределенный консенсус.
1.2	Основы криптографии: хеширование, хеш-функции, цифровые подписи, мультиподписи.
1.3.	Обзор рынка технологии блокчейн и платформ для разработки. Сферы применения технологии: государственный сектор, финансовая сфера, бизнес. Генерация бизнес-идей для создания блокчейн-проектов.
2	Разработка на платформах Ethereum, Bitcoin, Hyperledger и др
2.1	Блокчейн биткойна: история создания, принципы работы, консенсус в биткойне, майнинг, виды атак и угроз.
2.2	Введение в Ethereum и смарт-контракты. Сравнение с другими платформами: история создания платформы, сравнение блокчейна биткойна и Ethereum, понятия ETH и Gas, транзакции в Ethereum. Примеры простых контрактов. Токен-контракт. Применение блокчейна Ethereum
2.3	Изучение языка программирования Solidity и среды программирования. Синтаксис, простые типы данных, управление потоком выполнения кода Составные типы данных, доступ к данным транзакции или блока, встроенные криптографические функции, модификаторы видимости, автоматические гетеры, View и pure функции, Fallback функции, обработка исключительных ситуаций.
2.4	Разработка смарт-контрактов на платформе Ethereum. Наследование контрактов. Создание контрактов и вызов методов других контрактов. Библиотеки функций. Ассемблерные вставки для оптимизации контрактов. ERC 20 Token. Расширенное использование узла Ethereum
2.5	Разработка приложения на платформе Hyperledger: принципы работы платформы, модификация смарт-контрактов, настройка окружения.
3	Внедрение технологии блокчейн
3.1	Создание пилотных проектов в крупных компаниях России. Примеры реализованных проектов в финансовой сфере.

5 Образовательные технологии

Тренинг по генерации идей для бизнес-проектов

Встреча с представителем Национального расчетного депозитария Московской биржи

6 Оценочные средства для текущего контроля и аттестации студента

Примеры заданий для самостоятельного выполнения/решения для экзамена

1. Сгенерить идею проекта с применением технологии блокчейн.
2. Реализовать простой смарт-контракт для проведения транзакции.
3. Прописать архитектуру проекта с применением блокчейн-платформы Ethereum
4. Создать работающий прототип блокчейн-проекта (back-end).

Список теоретических вопросов к тесту

Вопросы по технологии распределенного реестра:

1. Выберите основные свойства технологии блокчейн?

Варианты ответов:

- Централизованная система
- Распределенная база данных
- Это публичность, данные доступны для всех в интернете
- Это безопасность, подделать или изменить записи невозможно
- Данные блокчейна хранятся в единственном месте

2. Что такое смарт-контракт?

Варианты ответов:

- Последовательность цифр и букв, которая даёт возможность любому, кто её знает, перечислить токены на любой счет
- Единица измерения криптовалюты
- Компьютерный алгоритм или условие, которое позволяет сторонам обмениваться активами
- Это документ, в котором прописана суть стартапа, выходящего на ICO

3. Что такое майнинг?

- Заработок за участие в работе блокчейна
- Создание новых блоков в цепочке и обработка транзакций
- Покупка криптовалют
- Процесс создания новых биткоинов, который построен на решении компьютерами сложных математических задач

4. Выберите неправильные факты о блокчейне

- Каждый член сообщества имеет доступ ко всей информации и истории
- Каждому пользователю присвоен адрес, состоящий из набора символов
- Участники блокчейна общаются через центральный узел
- Как только операция выполнена, записи о ней необратимы

5. Что обеспечивает работу и безопасность блокчейн?

7 Специальные программы криптографирования

8 Сложные математические алгоритмы

9 Владелец приватного ключа к системе

10 Мощные компьютеры, включенные в систему майнинга, между которыми распределена вся совокупность данных

10.1 Оценочные средства для оценки качества освоения дисциплины в ходе текущего контроля

Примерный перечень вопросов к различным формам текущего контроля. Вопросы для самопроверки студентов. Демонстрационные материалы для проведения текущего контроля (тестовые задания, кейсы, сценарии игр и пр.)

10.2 Примеры заданий промежуточной аттестации

Примеры вопросов, задач, заданий для зачета или экзамена, тренировочные тесты по дисциплине, демонстрационные материалы для проведения промежуточного контроля (тестовые задания, кейсы, сценарии игр и пр.)

11 Учебно-методическое и информационное обеспечение дисциплины

11.1 Основная литература

Bitcoin: A Peer-to-Peer Electronic Cash System, December 2008. Satoshi Nakamoto

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World), 2017. Дон Тапскотт, Алекс Тапскотт.

Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners. Chris Dannen

Just Enough Bitcoin for Ethereum

Ethereum White Paper. A Next-Generation Smart Contract and Decentralized Application Platform.

11.2 Дополнительная литература

Mastering Bitcoin: Programming the Open Blockchain, 2017. Andreas M. Antonopoulos

Mastering Ethereum, 2018. Andreas M. Antonopoulos, Gavin Wood.

Блокчейн изнутри. Как устроен Биткойн, Ethereum и смарт-контракты, 2017. Василий Зубарев.

Blockchain for Business - An Introduction to Hyperledger Technologies, 2017.

LinuxFoundationX

Blockchain for Finance with Python, 2017. Pawel Lachowicz

11.3 Программные средства

- Рекомендуемый язык программирования для освоения материала курса на практике – Python
- Рекомендуемая среда разработки – PyCharm Community Edition и (для работы в интерактивном режиме) IPython Notebook или Jupiter.
- Документация языка Python: <https://docs.python.org/2/>
- Руководство по Solidity на русском языке <https://github.com/ethereum/wiki/wiki/%5BRussian%5D-%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BF%D0%BE-Solidity>
- Стандарт токенов ERC20 https://theethereum.wiki/w/index.php/ERC20_Token_Standard

11.4 Дистанционная поддержка дисциплины

https://theethereum.wiki/w/index.php/Main_Page

<http://blockgeeks.com/>

<https://github.com/>

12 Материально-техническое обеспечение дисциплины

Проектор, компьютерный класс с установленным на каждый компьютер интерпретатором Python 2.x и Linux.

