

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор по цифровизации
образования**

Д.И. Гриц

	Рабочая программа дисциплины (модуля)
по дисциплине:	Программирование блокчейн
по направлению:	Бизнес-информатика
профиль подготовки:	Финансовые технологии и аналитика центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск" центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск"
курс:	2
квалификация:	магистр

Семестр, формы промежуточной аттестации: 4 (весенний) - Дифференцированный зачет

Аудиторных часов: 20 всего, в том числе:

лекции: 8 час.

семинары: 12 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 70 час.

Всего часов: 90, всего зач. ед.: 2

Программу составили:

Е.А. Савицкая, начальник отдела

О.А. Культепина, методист

Программа обсуждена на заседании центра дополнительного, дополнительного профессионального и онлайн-образования "Пуск" 13.06.2022

Аннотация

В рамках дисциплины «Программирование блокчейн» обучающиеся углубляют знания в блокчейн и криптографии, учатся программировать на блокчейн-платформах и знакомятся с проектами на Hyperledger Fabric и Ethereum.

1. Цели и задачи

Цель дисциплины

- формирование знаний и навыков в разработке блокчейн на примере экосистем Hyperledger Fabric и Ethereum.

Задачи дисциплины

- понимание принципов построения децентрализованных систем (алгоритмы консенсуса, криптография, расчет комиссии, тунинг нод) и структур данных хранения состояния блокчейна (Merkle tree, Patricia tree, Merkle Mountain Range и других);
- знание технологий и принципов сетевого взаимодействия (HTTP(s), RPC, gRPC, REST API);
- владение основными инструментами разработки и получение навыков разработки блокчейн-проектов;
- понимание принципов работы Hyperledger Fabric и Ethereum.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ПК-16 Способен готовить аналитические материалы для оценки мероприятий и выработки стратегических решений в области ИКТ	ПК-16.1 Эффективно применяет в ходе профессиональной деятельности методы и инструментарий анализа данных
	ПК-16.2 Знает методы подготовки аналитических материалов для оценки мероприятий и выработки стратегических решений в области ИКТ

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны знать:

- технологии блокчейн;
- P2P-сети;
- майнинг в блокчейн;
- особенности транзакций;
- шардинг;
- протоколы блокчейн;
- смарт-контракты;
- возможности масштабирования в блокчейн.

уметь:

- работать в среде Remix;
- работать с протоколами;
- работать с функциями в языках программирования блокчейн.

владеть:

- языком программирования Solidity в среде Remix;
- инструментами Cello, Composer;
- технологией создания проектов на платформе HyperLedger.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Введение в блокчейн-разработку и основы криптографии	2	2		10
2	Сетевой уровень взаимодействия и архитектура узла блокчейна	2	2		20
3	Ethereum	2	4		20
4	Hyperledger Fabric	2	4		20
Итого часов		8	12		70
Подготовка к экзамену		0 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 4 (Весенний)

1. Введение в блокчейн-разработку и основы криптографии

Криптография. Децентрализованный реестр. Протоколы консенсуса. Смарт-контракты. Протоколы анонимизации. Хеш-функции. Proof of work. Проблема двойных трат. Блоки и цепочки блоков. Дерево Меркла. Сложность майнинга. Награда за создание блока. Комиссии за транзакции. Тюнинг нод.

2. Сетевой уровень взаимодействия и архитектура узла блокчейна

Сетевые протоколы взаимодействия узлов. P2P-сети: примеры и отличия от архитектуры «клиент-сервер». Маршрутизация, bootstrapping P2P-клиента, announce vs request. Балансировка. Неструктурированные и структурированные оверлеи. Распределённые хеш-таблицы. Хранение файлов в P2P и атаки на P2P. BitTorrent. IPFS. Распространение информации в Bitcoin, разница в распространении транзакций и блоков, дополнительные relay-сети, протоколы исключения.

3. Ethereum

Базовая теория Эфириума. Виды узлов. Транзакции и смарт-протоколы. Газ. Язык программирования Solidity. Remix - онлайн среда разработки для Solidity. Выпуск смарт-контрактов в Remix. Вызов функций. Повторный запуск. контракта. Разные виды вызова выполнения функций (вызов, отправка транзакций). Подробности Solidity. Типы (struct, enum, mapping). Модификаторы view и pure. Видимость функций. Модификатор payable, fallback функции. Продвинутое смарт-контракты. Свойства блока и транзакций. Обработка ошибок (assert, require, revert и exceptions). Модификаторы функций. Наследование, интерфейсы. События. Библиотеки. Calls, delegated calls. Разбор существующих имплементаций. Возможности масштабирования. Шардинг. Предполагаемые решения Ethereum 2.0, альтернативные решения.

4. Hyperledger Fabric

История возникновения: Linux Foundation. Уровни Hyperledger – consensus, smart contract, communication, security/crypto, data stores, policy services, APIs и SDKs. Инструменты: Cello, Composer. Проекты на основе Hyperledger.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Занятия по учебной дисциплине проводятся с использованием дистанционных образовательных технологий. Каждый обучающийся обеспечен доступом к образовательной платформе <https://netology.ru/>.

6. Перечень рекомендуемой литературы

Основная литература

1. Блокчейн : Как это работает и что ждет нас завтра / А. Генкин, А. Михеев. — Москва, Альпина Паблишер, 2018.— URL: <https://e.lanbook.com/book/102775> (дата обращения: 30.12.2020). - Полный текст (Режим доступа : из сети МФТИ / Удаленный доступ)

Рекомендуемая литература для самостоятельного изучения:

- 1.Bitcoin: A Peer-to-Peer Electronic Cash System, December 2008. Satoshi Nakamoto
- 2.Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World), 2017. Дон Тапскотт, Алекс Тапскотт.
- 3.Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners. Chris Dannen
4. Just Enough Bitcoin for Ethereum
5. Ethereum White Paper. A Next-Generation Smart Contract and Decentralized Application Platform.

Дополнительная литература

1. Криптографические методы защиты информации [Текст] / С. М. Владимиров [и др.] ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т), Каф. радиотехники и систем управления - М.МФТИ,2016

Рекомендуемая литература для самостоятельного изучения:

1. Mastering Bitcoin: Programming the Open Blockchain, 2017. Andreas M. Antonopoulos
2. Mastering Ethereum, 2018. Andreas M. Antonopoulos, Gavin Wood.
3. Блокчейн изнутри. Как устроен Биткойн, Ethereum и смарт-контракты, 2017. Василий Зубарев.
4. Blockchain for Business - An Introduction to Hyperledger Technologies, 2017. LinuxFoundationX
5. Blockchain for Finance with Python, 2017. Pawel Lachowicz.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Язык Solidity: tutorialspoint.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

1. Образовательная платформа <https://netology.ru/>
2. Webinar.ru
3. GitHub
4. Zoom
5. Google Drive

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения дисциплины, уметь применять полученные знания для решения различных задач.

Успешное освоение курса требует:

- посещения всех занятий, предусмотренных учебным планом по дисциплине;
- ведения конспекта занятий;
- напряжённой самостоятельной работы студента.

Самостоятельная работа включает в себя:

- чтение рекомендованной литературы;
- проработку учебного материала, подготовку ответов на вопросы, предназначенных для самостоятельного изучения;
- решение задач, предлагаемых студентам на занятиях;
- подготовку к выполнению заданий текущей и промежуточной аттестации.

Показателем владения материалом служит умение без конспекта отвечать на вопросы по темам дисциплины.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к преподавателю.

Возможен промежуточный контроль знаний студентов в виде решения задач в соответствии с тематикой занятий.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Бизнес-информатика		
профиль подготовки:	Финансовые технологии и аналитика	▲	▲
	онлайн-образования "Пуск"	▲	▲
	онлайн-образования "Пуск"		
курс:	2		
квалификация:	магистр		

Семестр, формы промежуточной аттестации: 4 (весенний) - Дифференцированный зачет

Разработчики:

Е.А. Савицкая, начальник отдела

О.А. Культепина, методист

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ПК-16 Способен готовить аналитические материалы для оценки мероприятий и выработки стратегических решений в области ИКТ	ПК-16.1 Эффективно применяет в ходе профессиональной деятельности методы и инструментарию анализа данных
	ПК-16.2 Знает методы подготовки аналитических материалов для оценки мероприятий и выработки стратегических решений в области ИКТ

2. Показатели оценивания компетенций

В результате изучения дисциплины «Программирование блокчейн» обучающийся должен:

знать:

- технологии блокчейн;
- P2P-сети;
- майнинг в блокчейн;
- особенности транзакций;
- шардинг;
- протоколы блокчейн;
- смарт-контракты;
- возможности масштабирования в блокчейн.

уметь:

- работать в среде Remix;
- работать с протоколами;
- работать с функциями в языках программирования блокчейн.

владеть:

- языком программирования Solidity в среде Remix;
- инструментами Cello, Composer;
- технологией создания проектов на платформе HyperLedger.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Проводится в форме опроса по темам предыдущего занятия и в формате автоматически проверяемых тестов на платформе.

Примеры вопросов опроса:

1. Опишите алгоритм создания триггерных функций и триггеров.
2. Расскажите, как происходит горизонтальное и вертикальное шардирование.
3. Определите архитектурные модели блокчейн.
4. Перечислите этапы проектирования базы данных.
5. Назовите отличия OLTP- от OLAP-систем.
6. Определите преимущества и недостатки NoSQL-систем.
7. Расскажите об этапах проектирования хранилища данных.

8. Сравните подходы ETL и ELT.
9. Опишите организацию данных и задачи администрирования.
10. Расскажите, как предоставляется доступ.
11. Раскройте алгоритм определения ролей, доступа и резервного копирования для заданной базы данных.
12. Расскажите про тестирование таблиц, символов и защищенных данных.
13. Расскажите, в чем заключается нагрузочное тестирование.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Примерные типы итоговых заданий на дифференцированном зачете:

1. Разработайте смарт-контракт для Ethereum.
2. При условии X какое программное решение с использованием блокчейн будет наиболее эффективным (условия для решения вопросов даются отдельно преподавателем)
3. Используйте Hyperledger для проектирования X.
4. Опишите архитектуру узла блокчейн.
5. Опишите требования к системе.
6. Найдите ошибки в требованиях к системе.
7. Нарисуйте блок-схему взаимодействия узлов.
8. Опишите P2P-сети и архитектуру "клиент-сервер".
9. Подготовьте распределенные хеш-таблицы.
10. Нарисуйте блок-схему для транзакции.
11. Опишите алгоритм определения ролей.
12. Найдите ошибки в нагрузочном тестировании.

Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета у обучающихся есть 45 минут на выполнение задания. Зачет проводится в виде выполнения итогового задания.