Федеральное государственное автономное образовательное учреждение высшего образования
"Национальный исследовательский университет
"Высшая школа экономики"

Факультет компьютерных наук
Кафедра технологий моделирования сложных систем

Рабочая программа дисциплины
«Введение в технологию блокчейн»

для образовательной программы «Науки о данных»
направления подготовки 01.04.02 Прикладная математика и информатика
магистратура

Разработчик программы
Янович Ю.А., к.ф.-м.н., ст.преподаватель кафедры технологий моделирования сложных систем

Одобрена на заседании кафедры технологий моделирования сложных систем
«___»_____ 201_ г.

Зав. кафедрой технологий моделирования сложных систем
А.Н.Соболевский

Утверждена Академическим советом образовательной программы
«___»_____ 201_ г., № протокола_____

Академический руководитель образовательной программы
«Науки о данных» С.О.Кузнецов

Москва, 2018

1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает требования к образовательным результатам и результатам обучения студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих дисциплину «Введение в технологию блокчейн», учебных ассистентов и студентов направления подготовки 01.04.02 Прикладная математика и информатика, обучающихся по образовательной программе «Науки о данных».

Программа учебной дисциплины разработана в соответствии с:

- Образовательным стандартом НИУ ВШЭ по направлению подготовки 01.04.02 Прикладная математика и информатика;
- Образовательной программой «Науки о данных».
- Объединенным учебным планом университета по образовательной «Науки о данных», утвержденным в 2017г.

2 Цели освоения дисциплины

Целью освоения дисциплины является изучение технологии блокчейн (распределенного реестра) с акцентом на её математические и технические основы, а также прикладные аспекты. Курс предназначен для новичков, желающих познакомиться с данной технологией.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен знать, что такое блокчейн, таксономию блокчейнов, область их применимости и технологические ограничения, математические основы блокчейна, обладать базовыми навыками работы на платформах Этериум и Экзонум.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ОС ВШЭ	Уровень формирования компетенции	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции	Форма контроля уровня сформированности компетенции
Способность понимать и применять в исследовательской и прикладной деятельности аппарат блокчейна	ПК-1	РБ	Студент способен спроектировать блокчейн-приложение от формулировки прикладной задачи до технического описания	Стандартные (лекционно- семинарские). Самостоятельные внеаудиторные занятия.	Итоговый проект, итоговый экзамен
Способность проводить моделирование математических примитивов в веб-приложении Юпитер-ноутбук	ПК-9	СД	Студент способен моделировать криптографические примитивы и простейшие блокчейны в веб-приложении Юпитер-ноутбук	Стандартные (лекционно- семинарские). Самостоятельные внеаудиторные занятия.	Домашнее задание, итоговый экзамен

Компетенция	Код по ОС ВШЭ	Уровень формирования компетенции	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции	Форма контроля уровня сформированности компетенции
Способность применять язык Солидити среды Этериум для решения прикладных задач	ПК-10	СД	Студент создает умные контракты (программы) на языке Солидити	Стандартные (лекционно- семинарские). Самостоятельные внеаудиторные занятия.	Домашнее задание, итоговый экзамен
Способность применять фреймворк Экзонум для решения прикладных задач	ПК-10	СД	Студент создает умные контракты (программы) на фремворке Экзонум	Стандартные (лекционно- семинарские). Самостоятельные внеаудиторные занятия.	Домашнее задание, итоговый экзамен

4 Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к вариативной части цикла дисциплин программы.

Является курсом по выбору для студентов 2 года обучения специализаций «Технологии моделирования сложных систем» и «Интеллектуальные системы и структурный анализ» программы магистратуры «Науки о данных».

Изучение курса «Введение в технологию блокчейн» требует предварительных знаний по основам алгебры и алгоритмов, умения работы в Юпитер-ноутбук, базовых навыков в одном языке из C++, Java, Rust.

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы		Самостоятельная работа
			Лекции	Практич. занятия	
1	Основны блокчейна	26	4	4	18
2	Криптографические основы блокчейна	30	5	5	20
3	Умные контракты	40	5	5	30
4	Приватные блокчейны	46	4	8	34

5	Текущее состояние технологии блокчейн	48	8	2	28
	Итого	190	26	24	140

6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1	2	Параметры
Текущий (неделя)	Домашнее задание	4		
	Проект		1	
Итоговый	Экзамен		*	устный

Порядок формирования оценок по дисциплине

Преподаватель оценивает правильность выполнения домашних заданий студентов. Результирующая оценка по 10-ти балльной шкале за самостоятельную работу определяется перед итоговым контролем – $О_{дз}$ как среднее значение оценок за отдельные домашние задания. Задания, присланные с опозданием менее 30 дней и не менее 7 дней до экзамена, оцениваются с дополнительным множителем 0,5.

В середине курса студентам предлагаются темы исследовательских и программистских проектов. В конце курса производится их публичная защита, результирующая оценка по 10-ти балльной шкале за которые определятся как $О_{пр}$.

В диплом выставляется результирующая оценка по учебной дисциплине, которая формируется по следующей формуле, где $О_{экзамен}$ – оценка за ответ на устном экзамене:

$$О_{результ} = 0{,}3 \cdot О_{дз} + 0{,}3 \cdot О_{пр} + 0{,}4 \cdot О_{экзамен}.$$

Способ округления оценок: арифметический.

7 Содержание дисциплины

Тема 1. Основны блокчейна.

Блокчейн: определение, свойства и примеры индустриального применения. Блокчейн как технология в основе Биткоина. Таксономия блокчейнов. Моя игрушечная криптовалюта (практика). Препарируя Биткоин: сетевой протокол и клиенты.

Тема 2. Криптографические основы блокчейна.

Основы криптографии. Криптография с отрытым ключом, RSA. ElGamal. Эллиптические кривые. Инфраструктура криптографии с открытым ключом. Доказательства с нулевым разглашением. Схемы разделения секрета.

Тема 3. Умные контракты.

Микроплатежи и язык Биткоин скрипт. Блокчейн Этериум и умные контракты в нем. Лайтнинг технология.

Тема 4. Приватные блокчейны.

Византийский устойчивые алгоритмы консенсуса. FLP-невозможность. Типы сетей и примеры алгоритмов консенсуса в них. Приватные блокчейны: Экзонум и Гиперледжер. Разработка приватных блокчейнов: особенности, технологии, практика.

Тема 5. Текущее состояние технологии блокчейн.

Возможности, ограничения и задачи блокчейна. Proof-of-X. Приватность в блокчейнах: пример Биткоина. Приватность в блокченах: доказательства с нулевым разглашением и приватные умные контракты.

8 Учебно-методическое и информационное обеспечение дисциплины

1. Swan M. Blockchain: Blueprint for a new economy. – " O'Reilly Media, Inc.", 2015.
2. Katz J. et al. Handbook of applied cryptography. – CRC press, 1996.
3. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. – 2008.
4. Wood G. Ethereum: A secure decentralised generalised transaction ledger //Ethereum project yellow paper. – 2014. – Vol. 151. – P. 1-32.
5. Sasson E. B. et al. Zerocash: Decentralized anonymous payments from bitcoin //Security and Privacy (SP), 2014 IEEE Symposium on. – IEEE, 2014. – P. 459-474.
6. Yanovich Y., Mischenko P., Ostrovskiy A. Shared send untangling in bitcoin. – Working Paper, Bitfury Group Limited, 2016.
7. Prihodko P. et al. Flare: An approach to routing in lightning network //White Paper – 2016.
8. Ermilov D., Panov M., Yanovich Y. Automatic bitcoin address clustering //Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on. – IEEE, 2017. – P. 461-466.
9. Cachin C. Architecture of the Hyperledger blockchain fabric //Workshop on Distributed Cryptocurrencies and Consensus Ledgers. – 2016.
10. https://blockgeeks.com/guides/what-is-blockchain-technology/
11. https://bitcoin.org
12. https://github.com/bitcoin/bitcoin
13. https://ethereum.org/
14. https://github.com/ethereum/
15. https://exonum.com/
16. https://github.com/exonum

9 Оценочные средства для текущего контроля и аттестации студента

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

Вопросы для самопроверки студентов:

Тема 1. Основны блокчейна.

- Какие типы блокчейнов существуют?
- Что такое задача консенсуса?
- Какими свойствами обладает консенсус, основанный на доказательстве выполнения работы?

Тема 2. Криптографические основы блокчейна.

- Как устроен криптографический алгоритм с открытым ключом RSA?
- Сформулируйте задачу доказательства с нулевым разглашением.
- Как устроен алгоритм разделения секрета по схеме Шамира?

Тема 3. Умные контракты.

- Какие возможности есть в языке Биткоин скрипт?
- Как устроены микроплатежи в Биткоине?
- Как устроен язык Солидити?

Тема 4. Приватные блокчейны.

- Что такое византийски устойчивые алгоритмы консенсуса?
- Какие типы сетей и процессоров выделяют в задаче византийски устойчивого консенсуса?
- Архитектура фремворка Экзонум.

Тема 5. Текущее состояние технологии блокчейн.

- Как устроен консенсус с делегированным доказательством обладания долей?
- Какую блокчейн и оффчейн информацию можно извлечь о сети Биткион?
- Что такое приватный умный контракт?

9.2 Примеры заданий промежуточной аттестации

Примеры домашних заданий:

- Выборочно оценить вероятность двойной траты в заданной игрушечной криптовалюте на языке Python как функцию от сложности для различного фиксированного количества майнеров.
- Напишите умный контракт на Солидити для сдачи квартиры в аренду с расчётом в криптовалюте и страховкой от скачков обменного курса.
- Реализуйте цепь управления поставками для почтовых марок на фремворке Exonum.

Примеры экзаменационных вопросов:

- Блокчейн: определение, свойства, примеры.
- Доказательство выполнения работы в сети Биткоин.
- Криптографические хэш функции.
- Задача консенсуса. Теорема FLP.
- Микроплатежи и умные контракты.

9.3 Программные средства

Для успешного освоения дисциплины, студент использует следующие программные средства:

- Веб-приложение Jupyter notebook с базовым набором библиотек языка Python: numpy, matplotlib, socket.

- Клиент высокоуровневого языка для виртуальной машины Ethereum под названием Solidity (синтаксис похож на JavaScript), например, Geth, AlethZero или их веб-аналоги.
- Компилятор Rust.
- Компилятор Java.