Сколковский институт науки и технологий (Сколтех)

Рабочая программа дисциплины	**Введение в технологию блокчейн**

Преподаватель	Фролов Алексей Андреевич, профессор, д.ф-м.н.

Аннотация

Блокчейн (распределенный реестр), предложеный в 2008 как технология в основе криптовалюты Биткоин, нашёл применение во многих областях: государственные реестры, цепочки поставок, финансовый сектор, и другие. Блокчейн основан на красивых математических подходах из криптографии, структур данных и распределенных алгоритмах, таких как криптография с открытым ключом, Меркл деревья и протоколы консенсуса, а также ставит новые вызовы исследователям. В курсе будет рассказано, что такое распределенный реестр, какие теоретические принципы лежат в его основе, а также, какие тренды наблюдаются. Освоение материала требует лишь стандарных знаний студента направления компьютерных наук, а именно:
-) быть знакомым по крайне мере с одним высокоуровневым языком программирования и не бояться сталкиваться с новыми;
-) не пугаться возведения в степень над заданным полем ни на бумаге, ни на компьютере;
-) рисовать графики и выводить текст в Jupyter ноутбуках;
-) понимать, что такое алгоритм.

1. Основная информация

Академический уровень курса	Магистратура
Количество кредитов	3

Тип оценки - дифференцированная

Отображение оценок в процентах

A:	86
B:	76
C:	66
D:	56
E:	46
F:	0

2. Содержание курса

Тема	Краткое содержание	Лекции (час)	Семинары (час)	Лабораторные занятия (час)	Самостоятельная работа (час)
Базовое введение в блокчейн	Обзор технологии блокчейн, типы блокчейнов и промышленные примеры	5	3	5	7
Внедрение в системы баз данных	Различные типы систем баз данных, запросы, транзакции, распределенные системы баз данных, безопасность в них	2	3	3	10
Введение в криптографию	Типы шифров. Публичные и частные криптосистемы. Хэш-функция. Цифровые подписи и сертификаты. Инфраструктура открытых ключей. Обмен секретами, эзотерические протоколы, ментальный покер	3	2	5	10
Практический обзор блокчейн-технологий	Консенсус и невозможность достижения распределенного консенсуса при наличии одной ошибки процесса (теорема). Сетевые и вычислительные допущения (теорема). Свойства и примеры консенсуса. Атомарная трансляция. Tendermint. Exonum. Криптовалюта, сертификация, привязка. Промышленные примеры	1	3	6	13

3. Результаты обучения

Результаты обучения в Сколтехе указаны в соответствии со структурой результатов обучения в Сколтехе

1. ФУНДАМЕНТАЛЬНЫЕ ЗНАНИЯ
1.1. Знание математики и естественных наук
1.2. Знание прикладных и инженерных наук, включая современные
1.4. Междисциплинарное мышление, структура знаний и интеграция
2.1. ПОЗНАНИЕ И СПОСОБЫ РАССУЖДЕНИЯ
2.1.1. Аналитическое мышление и решение проблем
2.1.2. Системное мышление
2.1.3. Творческое мышление
2.2. ОТНОШЕНИЕ И ПРОЦЕСС ОБУЧЕНИЯ
2.2.3. Ответственность, интенсивность, настойчивость, безотлагательность и воля к достижению поставленных целей
2.2.4. Находчивость, гибкость и способность адаптироваться
2.3. ЭТИКА, СПРАВЕДЛИВОСТЬ И ДРУГИЕ ОБЯЗАННОСТИ
2.3.5. Активное видение и намерение в жизни
2.3.6. Приверженность социальному и профессиональному поведению
3.1. КОММУНИКАЦИЯ В МЕЖДУНАРОДНОЙ СРЕДЕ
3.1.1. Коммуникационная стратегия и структура
3.1.2. Письменная, электронная и графическая коммуникация

3.1.3. Устная презентация и обсуждение
3.1.4. Вопросы, слушание и диалог
3.1.5. Общение на английском языке в научной, деловой и общественной среде
3.1.6. Эффективное взаимодействие в различных культурных и международных условиях
3.2. КОМАНДНАЯ РАБОТА И ЛИДЕРСТВО
3.2.1. Формирование эффективных команд
3.2.2. Командная работа и управление проектами
3.2.5. Техническое и междисциплинарное сотрудничество
3.3. СОТРУДНИЧЕСТВО И ИЗМЕНЕНИЯ
3.3.1. Установление разнообразных связей и сетевого взаимодействия
3.3.5. Осуществление намеренных изменений
4.1. ПОНИМАНИЕ ГЛОБАЛЬНОГО СОЦИАЛЬНОГО, ЭКОЛОГИЧЕСКОГО И ДЕЛОВОГО КОНТЕКСТА
4.1.1. Осознавая потенциал и ограничения науки и техники, их роль в обществе и роль общества в их эволюции
4.1.3. Понимание технических продуктов, систем и инфраструктуры отрасли
4.1.5. Понимание бизнес—контекста - рынков, политики и экосистемы сектора
4.2. ДАЛЬНОВИДНОСТЬ — ИЗОБРЕТЕНИЕ НОВЫХ ТЕХНОЛОГИЙ ПОСРЕДСТВОМ ИССЛЕДОВАНИЙ
4.2.1. Процесс исследования — гипотеза, доказательства и защита
4.2.2. Фундаментальные исследования, ведущие к новым научным открытиям
4.2.3. Исследования, направленные на разработку новых технологий
4.3. ВИДЕНИЕ — РАЗРАБОТКА КОНЦЕПЦИИ И ПРОЕКТИРОВАНИЕ УСТОЙЧИВЫХ СИСТЕМ
4.3.1. Выявление потребностей и пожеланий заинтересованных сторон
4.3.2. Определение и формулирование целей и задач
4.3.4. Дисциплинарный и междисциплинарный дизайн для обеспечения устойчивости, безопасности, эстетики, работоспособности и других целей
4.3.5. Понимание технического контекста и экосистемы продукта или услуги
4.4. РЕАЛИЗАЦИЯ КОНЦЕПЦИИ — ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ
4.4.1. Проектирование и оптимизация устойчивого и безопасного внедрения и эксплуатации

4.5. РЕАЛИЗАЦИЯ КОНЦЕПЦИИ — ПРЕДПРИНИМАТЕЛЬСТВО И ПРЕДПРИИМЧИВОСТЬ НА ПРЕДПРИЯТИИ
4.5.4. Инициирование процессов проектирования и разработки
4.5.5. Продажа, маркетинг и дистрибуция продуктов и услуг
4.5.6. Понимание цепочки создания стоимости — инновационной системы, сетей и инфраструктуры

4.5.7. Управление интеллектуальной собственностью и соблюдение правовых процедур

4. Задания и выставление оценок

Требование к физической посещаемости (% от числа занятий)	85

Тип назначения	Краткое содержание задания	% от итоговой оценки за курс
Домашние задания	Три задания, посвященные Программированию и криптографии на основе блокчейна, все выполнены с использованием языка Python. Задания будут основаны на семинарских занятиях с акцентом на практическое применение и практический опыт. Участники двух заданий по блокчейну углубляются в программирование в рамках блокчейн-фреймворков, демонстрируя способность внедрять решения в децентрализованном контексте. Одновременно участники, выполняющие задание по криптографии, оттачивают свои навыки в использовании языка Python для решения криптографических задач.	30
Финальный экзамен	Будет представлен набор из четырех задач, составленных на основе заранее определенного набора вопросов, и задача состоит в том, чтобы рассмотреть и решить эти проблемы. Их эффективность будет оцениваться на основе качества и точности их решений.	35
Финальный проект	Проектное задание позволяет студентам выбрать тему, связанную либо с криптографией, либо с внедрением блокчейна. Например, проект, ориентированный на криптографию, предполагает реализацию детерминированного Тест на первичность AKS наряду с рандомизированными тестами Миллера–Рабина и Тесты Ферма. Цель состоит в том, чтобы сгенерировать большие простые числа и сравнить время выполнения этих алгоритмов. С другой стороны, проект, ориентированный на блокчейн, сосредоточен на создании системы регистрации документов на децентрализованной платформе. Это предполагает развертывание системы в любой тестовой сети и взаимодействие с ней через библиотеки Python или JS, такие как Web3py или Web3js. Студенты могут выбрать бизнес-кейс, например, свидетельства о браке или соглашения, и	35

	изучить такие функциональные возможности, как проверка действительности и подлинности документов, а также внедрение таких функций, как сроки годности. Во время презентации студентам предлагается продемонстрировать способы решения проблем в децентрализованной среде с использованием выбранного ими проекта.	

5. Критерии оценки

Задание 1 Типа	Домашние задания

Пример задания 1

Найдите сериализуемые истории в наборе транзакций, сгенерируйте секретный сеансовый ключ для Алисы и Боба в Протокол Диффи-Хеллмана, раскройте секрет, которым делится схема Блейкли
Разработайте и исследуйте реализацию функции проверки работоспособности, которая принимает заголовок текущего блока и сложность вычисления блока в качестве входных данных и возвращает одноразовый номер для этого блока и заголовок добытого блока.

Критерии оценки для задания 1

Учащиеся получают баллы в зависимости от результатов выполнения домашнего задания.
Максимальное количество баллов - 100.
Каждое задание дает равный вклад в итоговую оценку. Баллы за каждое задание зависят от его полноты.
Не выполненое задание - 0 баллов.
Задание выполнено полностью - ему соответствует максимальное количество баллов.

Задание 2 Типа	Финальный проект

Пример задания 2

Выберите одну тему из области криптографии или внедрения блокчейна.

Пример:

1. Простые числа играют важную роль в криптографии. К сожалению, до сих пор нет алгоритмов для генерации произвольных больших простых чисел, поэтому обычно мы генерируем большое случайное число и проверяем, простое оно или нет. В этом проекте мы попросим вас реализовать

детерминированный тест на простоту AKS, а также рандомизированные тесты Миллера–Рабина и Ферма. Кроме того, мы попросим вас сравнить время их выполнения.

2. Идея этого проекта заключается в создании регистрационного документа на децентрализованной платформе, документ может быть таким же простым, как свидетельство о браке или простые соглашения и т.д. Разверните его в любой тестовой сети и взаимодействуйте с ним через библиотеки python или JS (Web3py или Web3js). Вы можете развернуть его в своей локальной системе, где сможете взаимодействовать с ним и проверять состояние сертификата, т.е. является ли он подлинным, действительным или поддельным? кроме того, вы можете указать дату его действия (что-то вроде даты истечения срока действия). Это полностью зависит от вас, какое экономическое обоснование вы хотите использовать. Во время презентации возьмите любую проблему и покажите, как вы решили ее в децентрализованной среде с помощью этого проекта.

Критерии оценки для задания 2

Студенты создают проект в группе из 2 или 3 человек. Каждый студент в одной группе получает одинаковое количество баллов за проект.
Баллы начисляются в зависимости от результатов проекта.
Максимальное количество баллов - 100, и студент получает их за полностью завершенный и хорошо представленный проект. Если проект не завершен полностью или в нем есть слабые места, учащийся получает баллы, основанные на полноте и общем качестве проекта. Если проект не запущен, учащийся получает 0 баллов.

Задание 3 Типа	Финальный экзамен

Пример задания 3

Вам предлагаются четыре задачи:

1. Задача, основанная на криптографии (теория)
2. Задача математического решения криптографии.
3. Теоретическая задача о блокчейне, основанная на концепциях
4. Сценарий использования и реализация с использованием блокчейна (абзац).

Критерии оценки для задания 3

Максимальное количество баллов за каждый вопрос равно 1.
Каждое задание дает равный вклад в итоговую оценку. Баллы за каждое задание зависят от его полноты.
Невыполненная задача - 0 баллов.
Задание выполнено полностью - максимальное количество баллов, соответствующее ему.

6. Учебники и интернет-ресурсы

Необходимые учебники	ISBN-13 (or ISBN-10)
Lipton, Alexander, and Adrien Treccani. Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics. World Scientific, 2021.	9789811221538
B. Schneier Practical cryptography Wiley 2003	0471223573
Рекомендуемые учебники	
M.Swan Blockchain: Blueprint for a New Economy. O'REILLY 2015	978-1-491-92049-7
Документы	DOI or URL
Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. – Manubot, 2019.	https://columbia.github.io/ds2-class/papers/nakamotobitcoin.pdf
Buterin V. et al. Ethereum white paper: a next generation smart contract & decentralized application platform //First version. – 2014.	https://www.semanticscholar.org/paper/A-Next-Generation-Smart-Contract-and-Decentralized-Buterin/0dbb8a54ca5066b82fa086bbf5db4c54b947719a

Веб-ресурсы (ссылки)	Описание
https://en.bitcoin.it/wiki/Main_Page	Биткойн-вики
https://docs.ethhub.io/ethereumbasics/resources/	Содержит массу полезной информации
https://cryptozombies.io/	Интерактивные уроки для dApps

7. Оборудование

Программное обеспечение
iPython Visual Studio Code Jupyter Notebook

Оборудование
Персональные компьютеры

8. Дополнительные примечания

Предлагаемый курс 1) имеет четкое академическое содержание и требования к получению зачетных единиц, 2) соответствует результатам обучения по программе, 3) соответствует политике и регламенту Сколтеха.