Санкт-Петербургский государственный университет

Р А Б О Ч А Я П Р О Г Р А М М А
УЧЕБНОЙ ДИСЦИПЛИНЫ

Введение в блокчейн технологии
An Introduction to Blockchain Technologies

Язык(и) обучения

русский

Трудоемкость в зачетных единицах: 3

Регистрационный номер рабочей программы: 056866

Раздел 1. Характеристики учебных занятий

1.1. Цели и задачи учебных занятий

Основной целью освоения дисциплины «Введение в блокчейн технологии» является приобретение обучающимися знаний об основных понятиях, технологиях и способах применения технологии блокчейн, а также практических навыков работы с инструментами, применяемыми в области криптовалют.

Поставленная цель достигается путем решения следующих задач курса:

1) Ознакомить студентов с основными задачами, решаемыми в области криптовалют, базовыми алгоритмами этой области, а также со сферами практического применения данных алгоритмов;
2) Способствовать развитию практических навыков работы с реальными инструментами, применяемыми в области блокчейн;
3) Ознакомить с основными тенденциями развития подходов в данной области и нерешенными задачами в ней.

1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)

Дисциплина «Введение в блокчейн технологии» относится к циклу М.2 основной образовательной программы высшего образования «Технологии баз данных» по направлению 02.04.02 «Фундаментальные информатика и информационные технологии». Данная дисциплина входит в базовую часть учебного периода, рассчитана на изучение в первом семестре первого года обучения в магистратуре. Формой отчетности является зачет по изученному теоретическому материалу, темам семинаров и практическим заданиям, которые студенты выполняют в течение семестра.

Студент, обучающийся по данной дисциплине, должен иметь знания в теории вероятностей, дискретной математике, линейной алгебре, программировании.

1.3. Перечень результатов обучения (learning outcomes)

Дисциплина способствует формированию следующих компетенций:

ПКП-3 Способен творчески применять базовые знания математических и естественных наук, программирования и информационных технологий

ПКП-6 Способен применять основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений

ПКП-7 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

КП-02.2 Способен разрабатывать приложения баз данных, владеть алгоритмами и технологиями анализа данных

КП-02.3 Способен применять в профессиональной деятельности методы проектирования и оптимизации баз данных и технологии распределенных баз данных

В результате освоения курса обучающиеся должны

знать:

- ☐ основные криптографические структуры данных: хэш-указатели, блокчейн, деревья Меркла;
- ☐ структуру и организацию сети Bitcoin;
- ☐ альтернативные криптовалюты и иные применения технологии блокчейн;
- ☐ принципы работы Bitcoin Script;
- ☐ принципы распределенного и децентрализованного консенсуса;

уметь:

☐ уметь применять математический аппарат для анализа поведения распределенной сети;
☐ уметь реализовывать умные контракты в сети Ethereum;
владеть:
☐ владеть средствами для анализа транзакций в сети Bitcoin;
☐ практическими навыками работы с инструментами, применяемыми в области криптовалют.

1.4. Перечень и объём активных и интерактивных форм учебных занятий

При изложении части тем, по желанию лектора, применяется мультимедиа-проектор для проведения презентаций.
В рамках данного курса используются такие активные формы работы, как:
☐ подготовка к семинарским занятиям;
☐ подготовка доклада по предложенной преподавателем теме;
☐ выполнение индивидуальных заданий по реализации изученных алгоритмов;
интерактивные формы обучения:
☐ метод групповой работы при решении задач во время практических занятий;
☐ экспертная оценка другими обучающимися результатов решения индивидуальных заданий и коллективное обсуждение полученных результатов.
Общий объем активных и интерактивных форм учебных занятий составляет 28 часов.

Раздел 2. Организация, структура и содержание учебных занятий

2.1. Организация учебных занятий

2.1.1 профиль Технологии баз данных

Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся																		
Код модуля в составе дисциплины, практики и т.п.	Контактная работа обучающихся с преподавателем												Самостоятельная работа				Объём активных и интерактивных форм учебных занятий	Трудоёмкость
	лекции	семинары	консультации	практические занятия	лабораторные работы	контрольные работы	коллоквиумы	текущий контроль	промежуточная аттестация	итоговая аттестация	под руководством преподавателя	в присутствии преподавателя	сам. раб. с использованием методических материалов	текущий контроль (сам.раб.)	промежуточная аттестация (сам.раб.)	итоговая аттестация (сам.раб.)		
ОСНОВНАЯ ТРАЕКТОРИЯ																		
Форма обучения: очная																		
Семестр 1		18		14					2				50		24		18	3
		10-25		10-25					10-25				1-1		1-1			
ИТОГО		18		14					2				50		24			3

Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации						
Код модуля в составе дисциплины, практики и т.п.	Формы текущего контроля успеваемости		Виды промежуточной аттестации		Виды итоговой аттестации (только для программ итоговой аттестации и дополнительных образовательных программ)	
	Формы	Сроки	Виды	Сроки	Виды	Сроки
ОСНОВНАЯ ТРАЕКТОРИЯ						
Форма обучения: очная						

Семестр 1			зачёт, устно, традиционная форма	по графику промежуточной аттестации		

2.2. Структура и содержание учебных занятий

№ п/п	Наименование темы (раздела, части)	Вид учебных занятий	Количество часов
1	Биткоин	семинары	7
		практические занятия	4
		по методическим материалам	16
2	Расширения биткоина и другие криптовалюты	семинары	7
		практические занятия	3
		по методическим материалам	16
3	Блокчейн и его применение	семинары	4
		практические занятия	3
		по методическим материалам	17

Содержание учебных занятий

Тема 1. Биткоин (Bitcoin)

Семинары:

1. Введение в криптографию и криптовалюты. Предпосылки создания цифровых и криптовалют. Криптографические хэш-функции. Хэш-указатели и структуры данных. Блокчейн. Деревья Меркла. Цифровые подписи. Публичные клюи как идентификаторы. Примеры простых криптовалют.
2. Распределенный консенсус. Децентрализация. Proof-of-work. Криптографические загадки. Мотивация для справедливого поведения.
3. Протоколы Bitcoin. Транзакции. Bitcoin script. Приложения («зеленые адреса», гарант, микро-платежи, умные контракты). Блоки. Сеть Биткоин.
4. Применение Bitcoin и безопасность. Хранение биткоинов. Горячее и холодное хранилища. Разделение ключей. Комиссия за транзакции.
5. Добыча Bitcoin. Задачи майнеров. Сложность. Оборудование. Пулы. Стратегии майнеров и возможные атаки. Forking. Сокрытие блоков. Черные списки транзакций и кошельков.

Практические задания:

1. Провести транзакции в сети Bitcoin TestNet и в основной сети Bitcoin.
2. Реализовать нестандартные стратегии майнинга для повышения прибыли.

Тема 2. Расширения биткоина и другие криптовалюты

Семинары:

1. Альтернативные подходы к майнингу и распределенному консенсусу. Альтернативные криптографические загадки. Proof-of-Useful-Work. Proof-of-stake и виртуальный майнинг.
2. Анонимность и миксеры. Псевдонимы. Сторонние каналы идентификации. Анализ транзакций. Этика анонимности. Деанонимизация сети Биткоин. Миксеры. Децентрализованые миксеры. Zerocoin и Zerocash.
3. Сообщество Bitcoin. Консенсус о правилах. Форки. Реальный мир.
4. Обзор альтернативных криптовалют. История и мотивация. Виды добычи. Namecoin. Litecoin. Капитализация рынков. Введение в Ethereum
5. Разработка умных контрактов с Ethereum. Ethereum и DAO.

Практические задания:

1. Провести деанонимизацию пользователей биткоин, используя только информацию о транзакциях.

Тема 3. Блокчейн и его применение

Семинары:

1. Постквантовая криптография, segregated witness и aggregate signatures.
2. Умная собственность, инфопотоки и открытые источники случайных чисел.
3. Применение криптовалют и блокчейна в традиционных финансах.

Практические занятия:

1. Реализовать умные контракты в сети Ethereum: датский и английский аукционы.

Раздел 3. Обеспечение учебных занятий

3.1. Методическое обеспечение

3.1.1 Методические указания по освоению дисциплины

Самостоятельная проработка изученных на аудиторных занятиях материалов; выполнение практических заданий по изучаемым разделам; выбор темы для детального изучения, подготовка презентации по ней, выступление с докладом перед группой; выступление с презентацией перед группой; использование рекомендованной литературы и ресурсов в сети интернет.

3.1.2 Методическое обеспечение самостоятельной работы

Самостоятельная работа студентов в рамках дисциплины «Криптовалюты и технологии блокчейн» является важным компонентом обучения. Данной программой предусмотрены виды деятельности студента, которые направляются и корректируются преподавателем, и виды учебной деятельности, которые осуществляются студентом самостоятельно в рамках плана изучения данной учебной дисциплины. К группе видов и форм самостоятельной работы студентов относятся:

- ☐ подготовка к семинарским занятиям;
- ☐ подготовка доклада по предложенной преподавателем теме;
- ☐ выполнение индивидуальных заданий по реализации изученных алгоритмов.

Для организации самостоятельной работы студентов рекомендуется предоставить презентации с изучаемым материалом, проводить консультации во время аудиторных занятий.

3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания

По результатам освоения дисциплины студентам предлагается выполнить доклад по предложенной преподавателем теме.

Промежуточная аттестация проходит в форме собеседования по пройденному материалу, с учетом результатов выполнения индивидуальных заданий и/или доклада.

Оценка «зачтено» ставится при условии успешного выполнения не менее 50% практических заданий, а также наличия подготовленного доклада по одной из тем семинаров, знания основных определений и алгоритмов.

Оценка «зачтено» также может быть поставлена при отсутствии результатов практических заданий в случае ответа на два теоретических вопроса.

Обучающимся могут быть зачтены результаты освоения следующего онлайн курса:

1. Bitcoin and Cryptocurrency Technologies (Принстонский университет) https://www.coursera.org/learn/cryptocurrency (подтверждается сертификатом, сертификат участника или сертификат с отличием – оценка «зачтено»).

Преподаватель имеет право предоставить информацию о задолженностях студента в аттестационную комиссию.

3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)

Примерный перечень тем докладов:

1. Проблемы и ограничения существующего протокола Bitcoin;
2. Полностью анонимные криптовалюты на примере zkSNARKS и Zerocash;
3. Риски при работе с умными контрактами;
4. Как sidechains могут улучшить сеть Bitcoin.
5. Биткоин как платформа. Append-only log. Sidechains. Платежи вне блокчейна и сеть lightning. Умная собственность. Безопасные лотереи в Bitcoin. Общедоступный источник случайных чисел.

Список теоретических вопросов:

1. Предпосылки создания цифровых и криптовалют. Криптографические хэш-функции. Хэш-указатели и структуры данных.
2. Блокчейн. Деревья Меркла. Цифровые подписи. Публичные клюи как идентификаторы. Примеры простых криптовалют.
3. Распределенный консенсус. Децентрализация. Proof-of-work. Криптографические загадки.
4. Протоколы Bitcoin. Транзакции. Bitcoin script. Приложения («зеленые адреса», гарант, микро-платежи, умные контракты). Блоки. Сеть Биткоин.
5. Применение Bitcoin и безопасность. Хранение биткоинов. Горячее и холодное хранилища. Разделение ключей. Комиссия за транзакции.
6. Добыча Bitcoin. Задачи майнеров. Сложность. Оборудование. Пулы. Стратегии майнеров и возможные атаки. Forking. Сокрытие блоков. Черные списки транзакций и кошельков.
7. Альтернативные подходы к майнингу и распределенному консенсусу. Альтернативные криптографические загадки. Proof-of-Useful-Work. Proof-of-stake и виртуальный майнинг.
8. Анонимность и миксеры. Псевдонимы. Сторонние каналы идентификации. Анализ транзакций. Этика анонимности. Деанонимизация сети Биткоин. Миксеры. Децентрализованые миксеры. Zerocoin и Zerocash.
9. Сообщество Bitcoin. Консенсус о правилах. Форки.
10. Альтернативные криптовалюты. История и мотивация. Виды добычи. Namecoin. Litecoin. Капитализация рынков. Введение в Ethereum
11. Разработка умных контрактов с Ethereum. Ethereum и DAO.
12. Постквантовая криптография, segregated witness и aggregate signatures.
13. Умная собственность, инфопотоки и открытые источники случайных чисел.
14. Применение криптовалют и блокчейна в традиционных финансах.

3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса

Просим Вас заполнить анкету-отзыв по прочитанной дисциплине. Обобщенные данные анкет будут использованы для ее совершенствования. По каждому вопросу проставьте соответствующие оценки по шкале от 1 до 10 баллов (**обведите** выбранный Вами балл). В случае необходимости впишите свои комментарии.

15. Насколько Вы удовлетворены содержанием дисциплины в целом?

1 2 3 4 5 6 7 8 9 10

Комментарий_____

16. Насколько Вы удовлетворены общим стилем преподавания?

1 2 3 4 5 6 7 8 9 10

Комментарий_____

17. Как Вы оцениваете качество подготовки предложенных методических материалов?

1 2 3 4 5 6 7 8 9 10

Комментарий_____

18. Какой из разделов дисциплины Вы считаете наиболее полезным, ценным с точки зрения дальнейшего обучения и/или применения в последующей практической деятельности?

Комментарий_____

19. *Что бы Вы предложили изменить в методическом и содержательном плане для совершенствования преподавания данной дисциплины?*

Комментарий_____

Что запомнилось из курса лекций? _____

_____

Что показалось самым сложным?

_____

СПАСИБО!

3.2. Кадровое обеспечение

3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий

К проведению семинаров и практических занятий должны привлекаться преподаватели, имеющие ученую степень и/или ученое звание, опыт планирования и организации учебного процесса, или квалифицированные специалисты в этой предметной области.

3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом

Для технического обеспечения учебного процесса необходима возможность прибегать к помощи специалистов, ответственных за надлежащее функционирование компьютеров и программного обеспечения, а также за своевременное поддержание в рабочем состоянии другой используемой техники.

3.3. Материально-техническое обеспечение

3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий

Аудитории и помещения, предназначенные для проведения занятий по данной дисциплине должны отвечать санитарным нормам, предусмотренным Образовательным стандартом реализации программ высшего образования Санкт-Петербургского государственного университета.

В аудиториях требуется наличие компьютеризированных рабочих мест для проведения совместных практических работ и демонстрации материалов курса.

3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования

Минимально необходимый для реализации программы перечень материально-технического обеспечения включает: мультимедийный проектор для презентаций и демонстраций, компьютеры для проведения практических работ. Для проведения учебных

занятий аудитория также должна быть оборудована настенными досками для письма маркерами.

3.3.3 Характеристики специализированного оборудования

Нет специальных требований.

3.3.4 Характеристики специализированного программного обеспечения

При практической работе каждый обучающийся во время занятий и самостоятельной подготовки должен быть обеспечен рабочим местом в компьютерном классе с выходом в Интернет.

Необходим доступ к инструментам и библиотекам для разработки: Eclipse / NetBeans / IntelliJ IDEA / MS Visual Studio 2013 / Python.

3.3.5 Перечень и объёмы требуемых расходных материалов

Фломастеры цветные, губки, бумага формата А4, канцелярские товары, картриджи принтеров, диски, флеш-накопители и др. в объёме, необходимом для организации и проведения занятий, по заявкам преподавателей, подаваемым в установленные сроки.

3.4. Информационное обеспечение

3.4.1 Список обязательной литературы

1) Публикация Bitcoin: A Peer-to-Peer Electronic Cash System (https://bitcoin.org/bitcoin.pdf)

3.4.2 Список дополнительной литературы

1) Research Perspectives and Challenges for Bitcoin and Cryptocurrencies (http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf)
2) Книга Bitcoin and Cryptocurrency Technologies (https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf)

3.4.3 Перечень иных информационных источников

1) Bitcoin Developer Guide (https://bitcoin.org/en/developer-reference)
2) Bitcoin Wiki (https://en.bitcoin.it/wiki/Main_Page)
3) Библиография публикаций о Bitcoin (http://users.encs.concordia.ca/clark/biblio.php#bitcoin)
4) Ethereum Wiki (https://github.com/ethereum/wiki/wiki)
5) Официальный сайт электронной библиотеки The ACM Digital Library: http://dl.acm.org/
6) Официальный сайт электронной библиотеки IEEE Xplore Digital Library: http://ieeexplore.ieee.org
7) https://www.coursera.org/learn/cryptocurrency

Раздел 4. Разработчики программы

Найден Алексей Владимирович – – старший преподаватель
alexey.nayden@gmail.com
Блеканов Иван Станиславович к.т.н доценti.blekanov@spbu.ru