

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра теории упругости и вычислительной математики
имени академика А.С. Космодамианского

УТВЕРЖДАЮ:

проректор по научно-методической
и учебной работе

Е.И. Скафа

«21» апреля 2021 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Современные проблемы прикладной математики и информатики»
частично практико-ориентированная дисциплина

Направление подготовки:	01.04.02 Прикладная математика и информатика
Профиль подготовки:	Прикладная математика и информатика
Образовательная программа:	<u>Магистратура</u>
Квалификация:	Магистр
Форма обучения:	очная

Донецк 2021

УТВЕРЖДАЮ:

Декан факультета математики
и информационных технологий
И. А. Моисеенко



«20» апреля 2021 г.

Рабочая программа учебной дисциплины «Современные проблемы прикладной математики и информатики» составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от «10» января 2021г. № 13; Государственного образовательного стандарта высшего образования (ГОС ВО) Донецкой Народной Республики (ДНР) (проекта) по направлению подготовки 01.04.02 Прикладная математика и информатика; Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки Донецкой Народной Республики от 10.11.2017 г. № 1171 (с изменениями и дополнениями); учебного плана и основной профессиональной образовательной программы высшего образования направления подготовки 01.04.02 Прикладная математика и информатика, магистерской программы: «Прикладная математика и информатика», разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

доцент кафедры упругости и вычислительной математики
имени академика А.С. Космодамианского
канд. физ.-мат. наук

В. Н. Неспирный

Рабочая программа учебной дисциплины утверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского

Протокол № 15 от «12» апреля 2021 г.

Заведующий кафедрой

В.И. Сторожев

Рабочая программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий

Протокол № 4 от «14» апреля 2021 г.

Председатель учебно-методической комиссии
факультета математики и информационных технологий

Л.И. Селякова

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Современные проблемы прикладной математики и информатики» является частично практико-ориентированной дисциплиной и относится к базовой части образовательной программы. Для изучения данной учебной дисциплины необходимы знания и умения, формируемые *предшествующими дисциплинами* – «Основы информатики», «Теория вероятностей и математическая статистика», «Математические основы защиты информации», «Компьютерные сети», *сопутствующими дисциплинами* – «Современные методы криптографии». Знания и умения, полученные в ходе изучения дисциплины «Современные проблемы прикладной математики и информатики», являются основой для изучения курса «Распределенные информационные системы», используются при написании выпускной квалификационной работы.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины	Форма обучения	
	Очная	Заочная
Направление подготовки	01.04.02 Прикладная математика и информатика	
Магистерская программа	Прикладная математика и информатика	
Программа подготовки	Магистратура	
Квалификация	Магистр	
Количество содержательных модулей и тем	3 (18)	
Дисциплина базовой / вариативной части образовательной программы	Базовой части	
Формы контроля	1 модульный контроль, зачет в 1-м семестре	
Год подготовки	1	
Семестр	1	
Количество зачетных единиц	3	
Количество часов всего	108	
в т.ч.:		
- лекционных	18	
- практических или семинарских	18	
- лабораторных	-	
- самостоятельной работы	72	
в т.ч. индивидуальное задание	-	
Недельное количество часов	6	
в т. ч.: - аудиторных	2	
- самостоятельной работы студента	4	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Современные проблемы прикладной математики и информатики» – получение базового представления о предпосылках появления распределенных реестров, возможностях и основных приложениях технологии блокчейн, основных математических алгоритмах и ряде систем, в которых используется данная технология, в том числе при создании и функционировании криптовалют.

Задачи:

- усвоение теоретических основ и практических навыков работы с распределенным реестром и использования технологии блокчейн в сфере обеспечения платежных систем, а также для других технологических процессов;

- освоение фундаментальных принципов построения и функционирования криптовалют и других распределенных систем на основе технологии блокчейн;

- понимание основных алгоритмов консенсуса, их ключевые свойства и характеристики, а также их применение;
- приобретение навыков работы с электронным кошельком, разработки и реализации различных скриптов и получение представления о смарт-контрактах;
- развитие навыков самостоятельной работы и умений находить и перерабатывать дополнительную информацию в данной предметной области;
- развитие творческого, научного потенциала студентов, их познавательных интересов в области математического и технологического обеспечения современных финансовых технологий, стимулирование к дальнейшему занятию научной деятельностью.

Требования к результатам освоения дисциплины. Процесс изучения дисциплины «Современные проблемы прикладной математики и информатики» направлен на формирование элементов следующих **компетенций** в соответствии с ФГОС ВО РФ, ГОС ВО ДНР (проект) по направлению подготовки 01.04.02 Прикладная математика и информатика и основной профессиональной образовательной программы высшего образования направления подготовки 01.04.02 Прикладная математика и информатика, магистерской программы: «Прикладная математика и информатика»:

Универсальные компетенции (УК):

Наименование категории (группы) универсальных компетенций:

«Системное и критическое мышление»

УК-1

Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Наименование категории (группы) универсальных компетенций:

«Коммуникация»

УК-4

Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Общепрофессиональные компетенции (ОПК):

ОПК-1

Способен решать актуальные задачи фундаментальной и прикладной математики

ОПК-4

Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности

Профессиональные компетенции (ПК):¹

ПК-2

Способен проводить обработку и анализ научной информации и результатов исследований

ПК-6

Способен использовать современные методы разработки и реализации алгоритмов для решения задач профессиональной деятельности на базе языков программирования и пакетов прикладных программ

Индикаторы достижения компетенций и результаты обучения². Достижение

¹ Если ПК взята из профессионального стандарта – можно указать название профстандарта, кем и когда утвержден, регистрационный номер профстандарта

компетенций оценивается на основе таких индикаторов и соответствующих им результатов обучения:

Категории универсальных компетенций	Универсальные компетенции	Индикаторы	Результаты обучения
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Применяет системный подход и осуществляет критический анализ проблемной ситуации	Знает различие между институциональными и неинституциональными подходами к формированию и хранению критической информации
			Умеет различать типы составляющих архитектуры Blockchain-сети и их функциональные возможности
			Умеет ориентироваться в алгоритмах консенсуса и их особенностях
		УК-1.2. Разрабатывает стратегию действий для достижения поставленной цели	Знает базовые механизмы и алгоритмы функционирования распределенных реестров
			Знает сферы и особенности использования смарт-контрактов
			Умеет оценивать возможности использования распределенных реестров в рамках конкретных бизнес-моделей;
			Умеет использовать опыт применения систем электронных денег на практике
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Применяет информационно-коммуникационные технологии для академического и профессионального взаимодействия	Знает основные принципы и требования, предъявляемые к проектированию современных платежных систем
			Умеет осуществлять поиск необходимой информации на информационных ресурсах, в том числе на иностранном языке
			Владеет современными средствами информационно-коммуникационных технологий

Общепрофессиональные компетенции	Индикаторы	Результаты обучения
ОПК-1. Способен решать актуальные задачи фундаментальной и прикладной математики	ОПК-1.1. Осуществляет анализ научной литературы для выявления актуальных задач фундаментальной и прикладной математики	Знает специальную терминологию, связанную с созданием и применением на практике технологии блокчейн, криптовалют, смарт-контрактов и коллективного инвестирования;
		Умеет приобретать систематические знания из новой научной и учебной литературы по тематике распределенных реестров
	ОПК-1.2. Аргументированно обосновывает выбор метода решения конкретной актуальной задачи фундаментальной и прикладной математики на основе теоретических знаний	Знает возможности, преимущества и ограничения технологии распределенных реестров, а также перспективы их применения
		Владеет навыками нахождения аналогий между поставленной задачей и уже существующими решениями Владеет навыками эффективного общего анализа возможностей применения распределенных реестров для решения конкретных задач
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Использует и комбинирует существующие информационно-коммуникационные технологии для решения поставленных задач в области профессиональной деятельности с учетом требований информационной безопасности	Знает специальную терминологию, связанную с созданием и применением на практике технологии блокчейн, криптовалют, смарт-контрактов и коллективного инвестирования;
		Умеет приобретать систематические знания из новой научной и учебной литературы по тематике распределенных реестров
	ОПК-4.2. Адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности	Умеет использовать технологию блокчейн в разработке программных решений Владеет принципами построения Blockchain-сетей

Профессиональные компетенции	Индикаторы	Результаты обучения
ПК-2. Способен проводить обработку и анализ научной информации и результатов исследований	ИПК-2.1. Осуществляет сбор, обработку, систематизацию и оценку перспектив результатов научных исследований в области компьютерно-математического моделирования	Знает методологию научных исследований, основные научные понятия и проблемы, существующие в сфере распределенных реестров, криптовалют и смарт-контрактов.
		Знает принципы работы алгоритмов консенсуса;
		Знает самостоятельно анализировать и решать научно-исследовательские и инженерные задачи в области прикладной математики и информатики.
ПК-6. Способен использовать современные методы разработки и реализации алгоритмов для решения задач профессиональной деятельности на базе языков программирования и пакетов прикладных программ	ПК-6.3. Реализует существующие и/или модифицированные алгоритмы с помощью современных языков программирования и /или пакетов прикладных программ	Знает языки Bitcoin Script и Solidity
		Знает неинституциональные механизмы формирования распределенного доверия на базе распределенных реестров;
		Умеет реализовывать основные алгоритмы проверки транзакций
		Умеет различать понятия токена и криптовалюты;
		Владеет навыками взаимодействия с электронными кошельками

4. ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Дисциплина «Современные проблемы прикладной математики и информатики» предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельную работу студентов.

Материал излагается с использованием объяснительно-иллюстративных и эвристических методов преподавания. При проведении лекций и практических занятий используются персональные компьютеры, мультимедийные презентации, документация используемых программных средств и технологий, обозреватели блоков отдельных криптовалют.

В учебном процессе широко применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости. В учебном процессе используются интернет-ресурсы по данному курсу; рассматриваются задачи, максимально приближенные к конкретным практическим ситуациям, тесты, самостоятельная работа; контрольные работы.

Самостоятельная работа студентов предусматривает подготовку к практическим занятиям, подготовку конспектов и рефератов по отдельным вопросам изучаемых тем, изучение учебной и методической литературы.

Тематический план «Современные проблемы прикладной математики и информатики»

Темы	Вопросы темы
Содержательный модуль 1. Экономические основы и предпосылки создания криптовалют и технологии блокчейн	
1. Деньги и платежные системы. Виды платежных систем, история их развития	1.1. Бартерная, монетная, бумажная и чековая платежные системы: преимущества и недостатки. 1.2. Платежная система электронных кошельков. 1.3. Причины возникновения концепции криптовалюты.
2. Концепция криптовалют. Экономический аспект биткоина	2.1 Сущность биткоина как цифровой валюты и его свойства. 2.2. Формирование стоимости биткоина: спрос и предложение. 2.3. Социально-экономические факторы, влияющие на стоимость биткоина.
3. Виды систем управления	3.1. Понятие управления. 3.2. Виды систем управления: централизованная, децентрализованная и распределенная системы. 3.3. Преимущества и недостатки различных систем управления.**
4. Основы системы блокчейн	4.1. Концепция блокчейн. 4.2. Основные свойства и преимущества блокчейн.
5. Бизнес-среда структуры блокчейн	5.1. Бизнес-среда структуры блокчейн 5.2. Стадии процесса принятия и инвестиции
6. Модель автолизинга*	6.1. Основные элементы системы автолизинга 6.2. Модель автолизинга на основе блокчейн**
7. Значимые личности и компании системы блокчейн	7.1. Наиболее значимые личности в системе блокчейн. 7.2. Компании, использующие блокчейн**
Содержательный модуль 2. Архитектура и технологические аспекты распределенных реестров	
8. Криптографические основы криптовалют	8.1. Хеш-функции и цифровые подписи 8.2. Свойства хеш-функций и особенности применения на практике. 8.3. Примеры построения простых криптовалют
9. Механизмы децентрализации Биткоина	9.1. Децентрализация в сети Биткоин. 9.2. Механизмы достижения распределенного консенсуса. 9.3. Стимулирование узлов сети: плата за создание блока и транзакционная комиссия. 9.4. Понятие майнинга.
10. Транзакции Биткоина*	10.1. Транзакции биткоина. 10.2. Структура заголовка транзакции.** 10.3. Скриптовый язык биткоина и особенности его использования. 10.4. Реализация мультиподписи с использованием MULTISIG. 10.5. Примеры практического применения скриптов биткоина.** 10.6. Механизм присоединения новых узлов к сети. 10.7. Ограничения, существующие в сети Биткоин.**
11. Хранение и использование биткоинов	11.1. Способы хранения биткоинов: локальное хранение, холодное и горячее хранилища.

	<p>11.2. Способы разделения секретного ключа на части.</p> <p>11.3. Особенности работы с онлайн-кошельками, биткоин-биржами, платежными сервисами.**</p>
12. Особенности майнинга*	<p>12.1. Цели и сложности майнинга.</p> <p>12.2. Поколения аппаратного обеспечения для майнинга: центральные процессоры общего назначения, GPU, программируемые пользователем вентильные матрицы, ASIC.</p> <p>12.3. Экологические аспекты биткоин-майнинга.**</p> <p>12.4. Пулы совместного майнинга: цели создания и особенности распределения вознаграждения.</p> <p>12.5. Стратегии, применяемые майнерами.**</p>
13. Основы анонимности*	<p>13.1. Понятие анонимности.</p> <p>13.2. Способы увеличения анонимности в сети Биткоин.</p> <p>13.3. Децентрализованное и централизованное микширование.</p> <p>13.4. Анонимная коммуникационная сеть Tor.**</p>
<p align="center">Содержательный модуль 3. Социальные факторы блокчейна и криптовалют: механизмы регулирования, возможности применения, перспективы развития</p>	
14. Влияние общества, политики и законодательства на систему Биткоин	<p>14.1. Договоренности, на которых основана система Биткоин: договоренность о правилах, истории, ценности.</p> <p>14.2. Программное обеспечение Bitcoin Core.</p> <p>14.3. Механизмы регулирования системы Биткоин со стороны правительства.**</p>
15. Альтернативы Proof of Work*	<p>15.1. Особенности алгоритмов PoW и требования к ним.</p> <p>15.2. Альтернативные алгоритмы: алгоритмы с защитой от ASIC, алгоритмы, препятствующие объединению в пулы, социально полезные алгоритмы.</p> <p>15.3. Особенности вычисления Script.</p> <p>15.4. Виртуальный майнинг: достоинства, недостатки, перспективы развития.**</p>
16. Практика использования Биткоина в разных областях*	<p>16.1. Безопасное проставление штампа времени: особенности применения и реализации.</p> <p>16.2. Практическое применение свойств Биткоина: организация и проведение лотерей, билеты, цветные монеты.</p> <p>16.3. Сущность рынка прогнозов и анализ возможности его построения на базе Биткоина.**</p>
17. Экосистемы криптовалют	<p>17.1. Примеры альткоинов: неймкоин, лайткоин, пиркоин, догикоин.</p> <p>17.2. Способы сравнения альткоин-бирж и особенности их работы.</p> <p>17.3. Сущность совместного майнинга. Атомарные свопы как метод обмена разных альткоинов.</p>
18. Будущее Биткоина	<p>18.1. Статус системы блокчейн, перспективы развития.</p> <p>18.2. Умная собственность.</p> <p>18.3. Репрезентация и атомарность.</p> <p>18.4. Пути интеграции блокчейн: прямое использование блокчейн, встраивание, сайдчейн, альткоины.</p> <p>18.5. Реализация краудфандинга с помощью технологии блокчейн.**</p> <p>18.6. Преимущества и недостатки децентрализованных технологий в сравнении с традиционной системой.**</p>

* — практико-ориентированные темы.

** — вопросы, выносимые на самостоятельное изучение.

Структура дисциплины «Современные проблемы прикладной математики и информатики» по видам учебной деятельности

Названия содержательных модулей и тем	Количество часов							
	Очная форма обучения				Заочная форма обучения			
	Всего	в т.ч.			Всего	в т.ч.		
		Лекции	Практические	Самостоятельная работа		Лекции	Практические	Самостоятельная работа
Содержательный модуль 1. Экономические основы и предпосылки создания криптовалют и технологии блокчейн								
1. Деньги и платежные системы. Виды платежных систем, история их развития	6	1	1	4				
2. Концепция криптовалют. Экономический аспект биткоина	6	1	1	4				
3. Виды систем управления	6	1	1	4				
4. Основы системы блокчейн	6	1	1	4				
5. Бизнес-среда структуры блокчейн	6	1	1	4				
6. Модель автолизинга*	6	1	1	4				
7. Значимые личности и компании системы блокчейн	6	1	1	4				
Итого по содержательному модулю 1	42	7	7	28				
Содержательный модуль 2. Архитектура и технологические аспекты распределенных реестров								
8. Криптографические основы криптовалют	6	1	1	4				
9. Механизмы децентрализации Биткоина	6	1	1	4				
10. Транзакции Биткоина*	6	1	1	4				
11. Хранение и использование биткоинов	6	1	1	4				
12. Особенности майнинга*	6	1	1	4				
13. Основы анонимности*	6	1	1	4				
Итого по содержательному модулю 2	36	6	6	24				
Содержательный модуль 3. Социальные факторы блокчейна и криптовалют: механизмы регулирования, возможности применения, перспективы развития								
14. Влияние общества, политики и законодательства на систему Биткоин	6	1	1	4				
15. Альтернативы Proof of Work*	6	1	1	4				
16. Практика использования Биткоина в разных областях*	6	1	1	4				

17. Экосистемы криптовалют	6	1	1	4				
18. Будущее Биткоина	6	1	1	4				
Итого по содержательному модулю 3	30	5	5	20				
Всего часов	108	18	18	72				

5. ТЕМАТИКА ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Деньги и платежные системы. Виды платежных систем, история их развития.	1	
2.	Концепция криптовалют. Экономический аспект биткоина.	1	
3.	Виды систем управления.	1	
4.	Основы системы блокчейн	1	
5.	Бизнес-среда структуры блокчейн	1	
6.	Модель автолизинга	1	
7.	Значимые личности и компании системы блокчейн	1	
8.	Криптографические основы криптовалют	1	
9.	Механизмы децентрализации Биткоина	1	
10.	Транзакции Биткоина	1	
11.	Хранение и использование биткоинов	1	
12.	Особенности майнинга.	1	
13.	Основы анонимности	1	
14.	Влияние общества, политики и законодательства на систему Биткоин	1	
15.	Альтернативы Proof of Work	1	
16.	Практика использования Биткоина в разных областях	1	
17.	Экосистемы криптовалют	1	
18.	Будущее Биткоина	1	
Всего		18	

Темы практических занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Основные элементы системы Биткоин и блокчейн	1	
2.	Исследование структуры блокчейна с помощью Blockchain Explorer	1	
3.	Структура блока блокчейна Биткоин	1	
4.	Структура транзакций	1	
5.	Структуры данных для представления элементов блокчейна	1	
6.	Приложение Bitcoin Core и его возможности	1	
7.	Тестовые сети Биткоина	1	
8.	Клиентские приложения и их основные возможности	1	
9.	Алгоритмы хеширования семейства SHA	1	
10.	Шифрование с открытым ключом	1	
11.	Генерация ключей. Механизмы создания подписей	1	

12.	Задача Proof of Work. Оценка сложности	1	
13.	Майнинг	1	
14.	Получение истории транзакций и баланса транзакций	1	
15.	Криптовалюта Ethereum. Структура и операции в Ethereum	1	
16.	Смарт-контракты. Язык Solidity	1	
17.	Разработка смарт-контрактов в Remix IDE	1	
18.	Развертывание смарт-контрактов	1	
Всего		18	

6. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1.	Технология блокчейн и децентрализованные приложения	4	
2.	Приватные и публичные блокчейны	4	
3.	Сравнительная характеристика традиционных банковский онлайн-транзакций и транзакций в сети Биткоин	4	
4.	Полные ноды и облегченные кошельки в сети Биткоин	4	
5.	Блокчейн и его возможности	4	
6.	Токенизация и ICO	4	
7.	Формат ключей в Биткоин	4	
8.	Форки Биткоина	4	
9.	Хранение и обработка ключей в криптовалютных кошельках	4	
10.	Иерархическая генерация ключей	4	
11.	Pay-to-Script-Hash адреса и мультиподписи в Биткоин	4	
12.	Альтернативные форматы представления биткоин-адресов	4	
13.	Жизненный цикл транзакций	4	
14.	Протокол Segregated Witness	4	
15.	Обмен сообщениями между узлами Биткоин-сети	4	
16.	Технологии повсеместной токенизации	4	
17.	Виды атак и решения для их предотвращения в Биткоин	4	
18.	Методы построения криптографических обязательств	4	
Всего		72	

7. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Содержательный модуль 1. Экономические основы и предпосылки создания криптовалют и технологии блокчейн

1. Перечислите наиболее желательные свойства денег. Какими из этих свойств обладают деньги в различных платежных системах.
2. Должны ли деньги обязательно иметь внутреннюю стоимость?
3. В результате чего появляются долговые отношения в примитивных обществах?
4. Какие функции выполняют деньги в соответствии с законодательством о банковской системе?
5. С чем связана проблема двойной траты в системах электронных платежей и криптовалютах?
6. Назовите основные механизмы формирования стоимости криптовалют.

Содержательный модуль 2. Архитектура и технологические аспекты распределенных реестров

7. Опишите механизм одобрения транзакций в сети Биткоин.
8. В чем заключается идея распределенного консенсуса?
9. Укажите основные характеристики системы Биткоин, которые поддерживаются программным обеспечением и участниками сети.
10. Перечислите виды систем относительно типа управления, принятого в них. Укажите преимущества и недостатки каждого типа управления.
11. Перечислите основные требования, которые предъявляются к хеш-функциям.
12. Опишите механизм обязательств, построенных с использованием электронной подписи и хеша.
13. Что такое хеш-указатель и как он используется при формировании блоков?
14. Опишите структуру дерева Меркла и его основные свойства.

Содержательный модуль 3. Социальные факторы блокчейна и криптовалют: механизмы регулирования, возможности применения, перспективы развития

15. Опишите процесс майнинга, какую задачу должен решать майнер для получения вознаграждения?
16. В чем заключается идея холодного и горячего хранилища?
17. На чем основана концепция разделения ключей? Опишите ее механизм.
18. Перечислите преимущества и недостатки онлайн-кошелька.
19. Для чего майнеры объединяются в пулы и на каких принципах осуществляется их деятельность?
20. Приведите примеры кейсов в которых удобно использовать переадресацию, слепые подписи, зеленые адреса, микротранзакции, мультиподписи.

8. ОБРАЗЕЦ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Образовательная программа:	магистратура
Направление подготовки:	01.04.02 Прикладная математика и информатика
Магистерская программа:	Прикладная математика и информатика
Очная форма обучения.	
Семестр	1
Учебная дисциплина	Современные проблемы прикладной математики и информатики

Модульная контрольная работа

Часть 1. Вариант № 1

1. В каком году были определены и опубликованы протокол и принципы работы системы Биткоин?
2. Какой из видов платежных систем обеспечивает самую высокую скорость проведения платежей?
3. Перечислите преимущества и недостатки бартерной платежной системы.
4. В чем основной недостаток платежной системы электронных кошельков?
5. В каком случае транзакция в сети Биткоин считается одобренной?
6. Каким числом может выражаться величина платежа в системе Биткоин?
7. Перечислите основные социально-экономические факторы, влияющие на стоимость биткоина.
8. Охарактеризуйте процесс майнинга с точки зрения наличия конкуренции и типа управления.

9. Как называется власть или право отдавать приказы, принимать решения и требовать повиновения?
10. К какому типу систем относится банковская система Донецкой Народной Республики?
11. Назовите основные преимущества централизованных систем управления.
12. Охарактеризуйте систему блокчейн с точки зрения посредников, иерархии, доверия и режима доступа к информации (ее чтения/записи).
13. Где хранится информация о страховке машины в схеме автолизинга на основе блокчейн?
14. Что достоверно известно о личности Сатоши Накамото?
15. Чем занимается компания Lazooz?

Часть 2. Вариант № 1

1. Охарактеризуйте множество результатов вычисления хеш-функции.
2. Как называется свойство защищенной хеш-функции, которое исключает что кто-то из хеш-функции получит определенное выходное значение y ?
3. Что необходимо сделать злоумышленнику, если он хочет подделать данные в одном из блоков дерева Меркла?
4. Как должен поступить узел в рамках работы протокола распределенного консенсуса, если он получил блок, который содержит транзакции с корректными криптографическими подписями?
5. Укажите причины, по которым Биткойн способен достичь консенсуса на практике, вопреки тому, что в общем это довольно сложная задача?
6. Как в терминах сценариев проверяется то, что транзакция может быть успешно завершена?
7. Какие группы инструкций поддерживает скриптовый язык Биткойна?
8. Элис платит за услугу Бобу, используя микротранзакции. Если она внезапно отключится, не предупредив Боба, и перестанет пересылать оплату, что может сделать Боб в такой ситуации?
9. Как должны быть распределены средства между горячим и холодным хранилищем?
10. Биржа публикует валидную транзакцию с переводом 10 000 биткойнов сама на себя. Затем биржа подписывает случайно сгенерированную строку своим закрытым ключом, которым была подписана предыдущая транзакция в 10 000 биткойнов. Зачем это делается?
11. Какие основные факторы необходимо учитывать при определении рентабельности майнинга?
12. Что может означать несвязанность в Биткойн?
13. В каком случае пользователь сети Тог может потерять безопасность передачи информации по цепи маршрутизаторов?
14. Какой механизм использовал Шелковый путь, чтобы мотивировать участников на ведение честных сделок?
15. Перечислите требования к алгоритмам Proof of work.

9. КРИТЕРИИ ОЦЕНИВАНИЯ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

Номер задания	Количество баллов
часть 1, 1-15	по 1 баллу
часть 2, 1-15	по 2 балла
Всего	45 баллов

10. КРИТЕРИИ ОЦЕНИВАНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа (включая выполнение СРС и ИРС) оценивается в 40 баллов. В разрезе отдельных тем оценивание осуществляется следующим образом.

Оценивание СРС и ИРС по дисциплине «Современные проблемы прикладной математики и информатики»

Названия содержательных модулей и тем	СРС	ИРС
Содержательный модуль 1. Экономические основы и предпосылки создания криптовалют и технологии блокчейн		
1. Деньги и платежные системы. Виды платежных систем, история их развития	1	1
2. Концепция криптовалют. Экономический аспект биткоина	1	1
3. Виды систем управления	1	1
4. Основы системы блокчейн	1	1
5. Бизнес-среда структуры блокчейн	1	1
6. Модель автолизинга*	2	1
7. Значимые личности и компании системы блокчейн	1	1
Итого по содержательному модулю 1	8	7
Содержательный модуль 2. Архитектура и технологические аспекты распределенных реестров		
8. Криптографические основы криптовалют	1	1
9. Механизмы децентрализации Биткоина	1	1
10. Транзакции Биткоина*	1	2
11. Хранение и использование биткоинов	1	1
12. Особенности майнинга*	1	2
13. Основы анонимности*	2	1
Итого по содержательному модулю 2	7	8
Содержательный модуль 3. Социальные факторы блокчейна и криптовалют: механизмы регулирования, возможности применения, перспективы развития		
14. Влияние общества, политики и законодательства на систему Биткоин	1	1
15. Альтернативы Proof of Work*	1	2
16. Практика использования Биткоина в разных областях*	1	1
17. Экосистемы криптовалют	1	1
18. Будущее Биткоина	1	1
Итого по содержательному модулю 3	5	5
Всего баллов	20	20

11. КРИТЕРИИ ОЦЕНИВАНИЯ ОБЩЕЙ УСПЕВАЕМОСТИ

Общая оценка знаний студентов по дисциплине проводится по 100-балльной шкале согласно таким критериям, приведенным в таблице ниже. *Организационно-учебная работа студента* в аудитории оценивается на основе таких критериев как посещаемость занятий, активность во время проведения лекционных и практических занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала, решение задач и ситуаций у доски и т.п.).

Если зачетная дисциплина

Содержательные модули	Вид работы	Баллы
Содержательный модуль 1	Организационно-учебная работа студента в аудитории	5
	Самостоятельная работа	15
	Итого	20
Содержательный модуль 2	Организационно-учебная работа студента в аудитории	5
	Самостоятельная работа	15
	Итого	20
Содержательный модуль 3	Организационно-учебная работа студента в аудитории	5
	Самостоятельная работа	10
	Модульная контрольная работа	45
	Итого	60
Общий итог		100

Порядок оценивания учебных достижений обучающихся

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале	
		экзамен, дифференцированный зачет	зачет
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной аттестации	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в главном учебном корпусе университета (пр-кт Гурова, 6). Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя. Выход в Интернет проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, материально-техническую базу учебной лаборатории кафедры упругости и вычислительной математики имени академика А.С. Космодамианского.

13. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
1.	Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах / Даниэль Дрешер. – М.: ДМК Пресс, 2018. – 312 с.: ил.	0	-
2.	Генкин А, Алексей Михеев А. Блокчейн. Как это работает и что ждет нас завтра / Артем Генкин, Алексей Михеев. – М.: Издательство Альпина Паблишер, 2018. – 592 с.	0	-
3.	Романьков, В.А. Введение в криптографию. Курс лекций / В.А. Романьков. – 2-е изд., испр. и доп. – М.: ФОРУМ : ИНФРА-М, 2018. – 240 с.	0	-
<i>Дополнительная литература</i>			
4.	Свон М. Блокчейн: схема новой экономики / Мелани Свон. - М.: Олимп-бизнес, 2017. - 240 с., ил.	0	-
5.	Равал С. Децентрализованные приложения. Технология Blockchain в действии / С.Равал. – СПб.: Питер, 2017. – 240 с.: ил.	0	-
6.	Поппер Н. Цифровое Золото. Невероятная история биткойна или о том, как идеали-сты и бизнесмены изобретают деньги заново / Натаниэль Поппер. - М.: Диалектика, 2016. - 75 с.	0	-
7.	Винья П., Майкл Кейси М. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок / Пол Винья, Майкл Кейси. - М.: Издательство Манн, Иванов и Фербер. 2017. - 432 с.	0	-

14. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Онлайн-курс «Введение в криптовалюты и блокчейн» // Intuit.ru – URL: <https://www.intuit.ru/studies/courses/3443/685/info>
2. Онлайн-курс «Технологии криптовалют» // Intuit.ru – URL: <https://www.intuit.ru/studies/courses/3643/885/info>
3. Серия публикаций Bitcoin in a nutshell // Хабрахабр:
 - Cryptography - <https://habrahabr.ru/post/319868/>
 - Transaction - <https://habrahabr.ru/post/319860/>
 - Protocol - <https://habrahabr.ru/post/319862/>
 - Blockchain - <https://habrahabr.ru/post/320176/>
 - Mining - <https://habrahabr.ru/post/320178/>
4. Курс лекций от группы Distributed Lab // Youtube. – URL: https://www.youtube.com/playlist?list=PLhZQuKnA7yUBt82ow8rEfw_G8tNZjt3qB
5. Bitcoin Wiki – URL: <https://en.bitcoin.it/wiki/Introduction>
6. Официальная документация Bitcoin Core: <https://bitcoin.org/en/developer-documentation>
7. Bitcoin Whitepaper: <http://www.bitcoin.org/bitcoin.pdf>
8. Bitcoin's Academic Pedigree: <https://queue.acm.org/detail.cfm?id=3136559>

9. What is Blockchain Technology? A Step-by-Step Guide For Beginners
<https://blockgeeks.com/guides/what-is-blockchain-technology>
10. Blockchain: The Invisible Technology That's Changing the World
<https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor>
11. How a Bitcoin Transaction Works <https://www.ccn.com/bitcoin-transaction-really-works/>
12. A Gentle Introduction to Blockchain Technology <https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/>
13. On Public and Private Blockchain <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
14. What is Cryptocurrency. Guide for Beginners <https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies#accept-as-payment-for-business>
15. 2017 Was Bitcoin's Year. 2018 Will Be Ethereum's <https://www.coindesk.com/2017-bitcoins-year-2018-will-ethereums/>
16. What is Cryptocurrency: Everything You Need To Know
<https://blockgeeks.com/guides/what-is-cryptocurrency/>
17. Smart Contracts: The Blockchain Technology That Will Replace Lawyers
<https://blockgeeks.com/guides/smart-contracts/>
18. Introduction to Smart Contracts <http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html>
19. What is Ethereum? <http://ethdocs.org/en/latest/introduction/what-is-ethereum.html>
20. Smart Contracts: A White Paper <https://github.com/ethereum/wiki/wiki/White-Paper>
21. Account Management <http://ethdocs.org/en/latest/account-management.html>
22. Native: Account management <https://github.com/ethereum/go-ethereum/wiki/Native:-Account-management>
23. How Ethereum Works <https://www.coindesk.com/information/how-ethereum-works/>
24. What Is Meant By The Term “Gas”? <https://ethereum.stackexchange.com/questions/3/what-is-meant-by-the-term-gas>
25. Vitalik Buterin Doubles Down on Ethereum Incentive Strategy
<https://www.coindesk.com/vitalik-buterin-doubles-ethereum-incentive-strategy>
26. Blockchain Info <https://blockchain.info/>
27. Bitcoin Block Explorer <https://blockexplorer.com/>
28. Etherscan <https://etherscan.io/>

15. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Веб-браузер Google Chrome (Лицензия – бесплатное программное обеспечение с открытым исходным кодом) – URL: <https://www.google.com/intl/ru/chrome/>
2. Bitcoin Core (свободный проект с открытым исходным кодом, лицензия MIT) – URL: <https://bitcoin.org/ru/download>
3. Remix IDE (свободный проект с открытым исходным кодом, лицензия MIT) – URL: <https://remix.ethereum.org>