МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра общей и космической физики

УТВЕРЖДАЮ
Декан физического факультета
_____ Н.М. Буднев
«20» апреля 2023 г.

Рабочая программа дисциплины

Наименование дисциплины (модуля): Б1.В.ДВ.01.01 Распределенные базы данных. Блокчейн

Направление подготовки: 03.04.02 Физика

Направленность (профиль) подготовки: Астрофизика высоких энергий

Квалификация выпускника: магистр

Форма обучения: очная

Согласовано с УМК физического факультета
Протокол №38 от «18» апреля 2023 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой:
общей и космической физики
Протокол № 8
от «15» марта 2023 г.
Зав.кафедрой д.ф.-м.н., профессор
_____ Паперный В.Л.

Иркутск 2023 г.

Содержание

I. Цели и задачи дисциплины (модуля)

Развитие цифровых технологий привело к изменению концепции хранения и обработки данных в сети. Одним из современных направлений стала разработка NoSQL баз данных. При создании такой базы данных не требуется соблюдения формальных правил разработки таблиц. Информация хранится в так называемых плоских файлах в виде пар «параметр-значение».

Курс знакомит с современными методами хранения и обработки данных на примере распределенной базы данных – блокчейна. Информация в этой базе данных сохранена в непрерывной последовательной цепочке блоков, связанных между собой.

Разобраны криптографические алгоритмы, применяемые для блокчейна, рассмотрено создание и функционирование блокчейна на примере криптовалют. Приведены примеры программирования работы сети, обслуживающей криптовалюту.

II. Место дисциплины (модуля) в структуре ОПОП ВО

Курс рассчитан на магистрантов физических специальностей университетов. Является продолжением информатики, которую студенты усваивают на младших курсах и курса «Базы данных». Таким образом, обеспечивается непрерывность компьютерного образования. Занятия рассчитаны на один семестр.

Практические занятия предполагают работу на компьютерах и включают знакомство с криптографическими алгоритмами и работой в сети.

Курс «Распределенные базы данных. Блокчейн» относится к части, формируемой участниками образовательных отношений. Он изучается в третьем семестре на втором курсе магистратуры.

III. Требования к результатам освоения дисциплины

Курс «Распределенные базы данных. Блокчейн», с учетом положений федерального государственного образовательного стандарта высшего образования при подготовке магистра по направлению 03.04.02 Физика, позволяет студенту приобрести следующие компетенции:

- Способен выполнять математическую и компьютерную обработку, интерпретацию и анализ результатов астрофизических исследований (ПК-3).

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-3	*ИДК $_{ПК.3.3}$*	Знать: принципы построения распределенных баз данных на основе блокчейна, основные методы проектирования этих баз данных и их применения для хранения данных в сети. Уметь: проектировать и программировать эти системы и использовать их для хранения данных. Владеть: инструментами программирования блокчейна и навыками грамотного использования существующих систем криптовалют

IV. Содержание и структура дисциплины (модуля)

Объем дисциплины составляет 5 зачетных единицы, 180 часов,

в том числе 82 часа контактной работы.

Занятия проводятся только в очной форме обучения. Электронной и дистанционной форм обучения не предусматривается.

На практическую подготовку отводится 18 аудиторных часов (во время выполнения практических работ).

Форма промежуточной аттестации: зачёт.

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации *(по семестрам)*
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекции	Семинарские/ практические/ лабораторные занятия	Консультации		
1	2	3	4	5	6	7	8	9	10
1	*Раздел 1. Алгоритмы хеширования.*	3	10.2	3	4	6	0,2		Опрос
2	*Раздел 2. Криптография на эллиптических кривых*	3	22.2	3	4	6	0,2	12	Собеседование
3	*Раздел 3. Алгоритм вычисления открытого и закрытого ключа*	3	20.2	2	4	4	0,2	12	Собеседование
4	*Раздел 4. Создание нового блока. Майнинг*	3	22.2	4	4	6	0,2	12	Собеседование
5	*Раздел 5. Создание транзакции. Проверка правильности транзакции*	3	22.2	4	4	6	0,2	12	Собеседование
6	*Раздел 6. Технология P2P. Схема работы узла сети*	3	18.2	2	4	4	0,2	10	Собеседование
7	*Раздел 7. Структура блока Биткоин*	3	16.2		4		0,2	12	Собеседование
8	*Раздел 8. Хеширование транзакций. Подтверждение транзакций.*	3	24.2	2	4	4	0,2	16	Собеседование
9	*Раздел 9. Биткоин-кошелек и биткоин-адрес*	3	14.2		2		0,2	12	Собеседование
10	*Раздел 10. Алгоритм доказательства работы. Форки блокчейна*	3	2.2		2		0,2		Опрос
	Зачёт								
	КСР		**4**						
	КОнтроль		**4**						
Итого часов			**180**		**36**	36	**2**	98	

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
3	**Криптография на эллиптических кривых**	Самостоятельное изучение теоретического материала	В течение семестра	18	Опрос	[1,2,4]
3	**Знакомство с модулярной арифметикой и длинной арифметикой**	Самостоятельное выполнение заданий во время лабораторной работы	В течение семестра	18	Готовая программа	[1,2,4]
3	**Структура блокчейна**	Самостоятельное изучение теоретического материала	В течение семестра	22	Опрос	[1,3,4]
3	**Проверка транзакций**	Самостоятельное изучение теоретического материала	В течение семестра	18	Опрос	[1,3,4]
3	**Работа в интернете с информацией о сети биткоина**	Самостоятельное выполнение заданий во время лабораторной работы	В течение семестра	18	Демонстрация работы на сайте	[1]
3	**Подготовка к зачёту**	Работа с лекционным материалом и учебной литературой	К концу семестра	4	Собеседование	[1-4]
Общий объем самостоятельной работы по дисциплине (час)				**98**		

4.3. Содержание учебного материала

Раздел 1. Криптографические алгоритмы.

Тема 1. Алгоритмы хеширования. Алгоритм хеширования SHA256. Алгоритм хеширования RIPEMD160.

Тема 2. Криптография на эллиптических кривых. Непрерывная группа точек на эллиптической кривой. Дискретная группа точек. Модулярная арифметика. Длинная арифметика. Циклическая подгруппа.

Тема 3. Электронный кошелек. Алгоритм вычисления открытого и закрытого ключа. Создание электронного адреса. Кодировка Base58Check. Электронная подпись. Проверка подписи.

Раздел 2. Учебная криптовалюта.

Тема 4. Структура блока. Создание нового блока. Майнинг.

Тема 5. Транзакции. Структура транзакции. Создание транзакции. Проверка правильности транзакции.

Тема 6. Структура сети для работы с блокчейном. Технология P2P. Схема работы узла сети.

Раздел 3. Биткоин.

Тема 7. Структура блока. Генезис – блок.

Тема 8. Транзакции. Хеширование транзакций. Подтверждение транзакций.

Тема 9. Биткоин-кошелек и биткоин-адрес.

Тема 10. Майнинг. Алгоритм доказательства работы. Форки блокчейна.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	**2**	**3**	**4**	**5**	**6**	**7**
1.	Тема 1	Алгоритмы вычисление хеша	6	6	собеседование.	ПК-3.3.
2.	Тема 2	Эллиптические кривые. Группа точек	6	6	собеседование.	
3.	Тема 3	Цифровая подпись	4	4	собеседование.	
4.	Тема 4	Майнинг	6	6	собеседование.	
5.	Тема 5	Транзакции	6	6	собеседование.	
6.	Тема 6	Работа в локальной сети	4	4	собеседование.	
7.	Тема 8	Работа в интернете	4	4	собеседование.	

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1.	Криптография на эллиптических кривых	Самостоятельное изучение теоретического материала	Углубить свои знания по данной теме	[1,2]	18
2.	Знакомство с модулярной арифметикой и длинной арифметикой	Самостоятельное выполнение заданий во время лабораторной работы	Написать программу	[4]	18
3.	Структура блокчейна	Самостоятельное изучение теоретического материала	Углубить свои знания по данной теме	[1]	22
4.	Проверка транзакций	Самостоятельное изучение теоретического материала	Самостоятельное изучение теоретического материала	[3]	18
5.	Работа в интернете с информацией о сети биткоина	Самостоятельное выполнение заданий во время лабораторной работы	Освоить работу на сайте	[1,2]	18
6.	Подготовка к зачету				4

4.4. Методические указания по организации самостоятельной работы студентов

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в лабораторных экспериментах, выполнение контрольных заданий, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Самостоятельная работа реализуется:

1) Непосредственно в процессе аудиторных занятий - на практических занятиях, при выполнении лабораторных работ.
2) В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

3) В библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных и творческих задач.

Границы между этими видами работ достаточно размыты, а сами виды самостоятельной работы пересекаются. Таким образом, самостоятельной работа студентов может быть как в аудитории, так и вне ее.

4.5. Примерная тематика курсовых работ (проектов) (при наличии)

Курсовые проекты не предусмотрены.

V. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) *перечень литературы*

основная литература

1. Красов, В.И. Распределение базы данных Блокчейн [Текст] : учеб. пособие / В. И. Красов ; Иркут. гос. ун-т, Физ. фак. - Иркутск : Изд-во ИГУ, 2020. - 118 с. : ил., табл. ; 20 см. - Библиогр.: с. 107. - ISBN 978-5-9624-1848-3 – (20 экз.)

дополнительная литература

1. Макшанов, А. В. Большие данные. Big Data [Текст] : учебник / А. В. Макшанов, А. Е. Журавлев, Л. Н. Тындыкарь. - СПб. : Лань, 2021. - 184 с. : ил. ; 24 см. - (Высшее образование). - Библиогр.: с. 181-184. - ISBN 978-5-8114-6810-2. – (11 экз).

Справочная литература

1. Брюс Шнайер. Прикладная криптография [Текст] : протоколы,алгоритмы,исход.тексты на языке Си / Б. Шнайер. - М. : Триумф, 2003. – 815 с. – (1 экз).

2. Элементарное введение в эллиптическую криптографию [Текст] / А. А. Болотов [и др.]. - Изд. стер. - М. : Ленанд, 2020 - . - 21 см. - (Основы защиты информации ; № 3). Кн. 1 : Алгебраические и алгоритмические основы. - 2020. – 375 с. – (1 экз).

3. *Andrea Corbellini*. Elliptic Curve Cryptography [Электронный ресурс]. – URL: http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/. Перевод – https://habr.com/ru/post/335906/
4. Антонопулос А.М. Осваиваем биткоин. Программирование блокчейна / пер. с англ. А.В.Снастина. – М.: ДМК Пресс, 2018. – 428с.
5. *Lauri Hartikka*. Naivecoin: a tutorial for building a cryptocurrency [Электронный ресурс]. https://lhartikk.github.io/jekyll/update/2017/07/14/chapter1.html
6. *S. Nakamoto*, Bitcoin Whitepaper. [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf - (Дата обращения: 17.07.2019)
7. Protocol documentation [электронный ресурс]. – URL: https://en.bitcoin.it/wiki/Protocol_documentation

б) *периодические издания*

- нет.

в) *список авторских методических разработок*

1. *В.И.Красов*. Распределенные базы данных. Блокчейн. — Иркутск: изд. ИГУ, 2020. – 118 с. - Режим доступа: ЭЧЗ "Библиотех". - Неогранич. доступ.

2. В системе образовательного портала ИГУ (http://educa.isu.ru/) размещены методические материалы и задания по данному курсу.

г) *базы данных, информационно-справочные и поисковые системы*

документация, описание и примеры работы Блокчейн:

- https://blockgeeks.com/guides/what-is-blockchain-technology/
- https://bitcoin.org
- https://github.com/bitcoin/bitcoin
- Blockchain University - - https://www.youtube.com/channel/UCJ5uHx90mZGlK0lC-GSmtzw

- Blockchain Workshops? - https://www.youtube.com/channel/UC9Lmf5FfNkSmYMoxhQh5ktA/feed
- Что такое блокчейн-технология? - https://bitnovosti.com/2017/03/02/chto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1
- • ЭЧЗ «Библиотех» https://isu.bibliotech.ru/
- • ЭБС «Лань» http://e.lanbook.com/
- • ЭБС «Руконт» http://rucont.ru
- • ЭБС «Айбукс» http://ibooks.ru

Справочные материалы:

1. *Lauri Hartikka*. Naivecoin: a tutorial for building a cryptocurrency [Электронный ресурс]. https://lhartikk.github.io/jekyll/update/2017/07/14/chapter1.html
2. *S. Nakamoto*, Bitcoin Whitepaper. [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf - (Дата обращения: 17.07.2019)
3. Protocol documentation [электронный ресурс]. – URL: https://en.bitcoin.it/wiki/Protocol_documentation
4. Buterin V.et al.A next-generation smart contract and decentralized application platform //white paper. –2014. URL:https://github.com/ethereum/wiki/wiki/White-Paper (accessed 29 October 2018)

VI. Материально-техническое обеспечение дисциплины (модуля)

6.1. Учебно-лабораторное оборудование:

Применять полученные знания на практике студенты могут в специальном дисплейном классе с современной вычислительной техникой и соответствующим программным обеспечением. В классе имеет 14 стационарных компьютеров (Intel Atom CPU D2500) с мониторами (Samsung S19A10 18.5"), WiFi-роутер 54M Wireless Router TL-WR542G, маршрутизатор DES-1005D. Компьютеры имеют доступ к локальной сети университета и выход в Интернет. Студенты могут самостоятельно закреплять полученный материал в этих классах. На занятиях могут использоваться мультимедийные средства: переносной проектор (CASIO XJ-A241), стационарный настенный экран (Classic Solution, 244x244), ноутбук Lenovo B590. Кроме того, на факультете имеется компьютеризированная аудитория, предназначенная для самостоятельной работы.

6.2. Программное обеспечение:

На каждом компьютере установлены ОС Linux (Ubuntu 14.04.2 LTS) и следующие программные пакеты: Geany 1.23.1, Midnight Commander, Leafpad, Mozilla, Gnuplot, Evince 3.10.3, LibreOffice 4.2.8.2. Все установленное программное обеспечение Freeware.

На стационарных компьютерах в учебной аудитории дополнительно к Linux установлена операционная система MS Windows XP 5.1.2600.2. (55683-OEM-0013514-73984). На ноутбуках – Windows 8 (WIN8 EM – встроенная операционная система от производителя). А также стандартные средства MS Office для работы методическими материалами. Программа просмотра документов в PDF формате – Adobe Acrobat Reader (условия правообладателя, бессрочно).

6.3. Технические и электронные средства:

Во время лекционных занятий студентам демонстрируются на экране дополнительные и вспомогательные материалы (презентации, примеры использования программных кодов)

VII. Образовательные технологии

Контроль знаний производится во время собеседования после выполнения практической работы по соответствующей теме.

Для допуска к итоговому зачёту от студента требуется выполнить как минимум одно задание по каждому разделу курса.

Изучение данного курса идет в плане накопительной системы, т.е. содержательная часть каждого раздела, как правило, завершается опросом во время выполнения практической работы по соответствующей теме.

VIII. Оценочные материалы для текущего контроля и промежуточной аттестации

8.1. Оценочные материалы (ОМ)

Фонд оценочных средств (ФОС) представлен в приложении.

8.1.1. Оценочные средства для входного контроля

Входной контроль не осуществляется.

8.1.2. Оценочные средства текущего контроля

Контроль за работой студентов осуществляется посредством собеседования при защите ими отчетов по лабораторным работам.

Ниже приведены задания к некоторым разделам программы.

Задания к разделу 1

1. Написать программу, вычисляющую хеш от произвольного текста по адгоритму SHA256, сравнить с образцом, рассчитанным online – калькулятором в интернете.
2. Написать программу, вычисляющую хеш от произвольного текста по формату RIPMD160, сравнить с образцом, рассчитанным online – калькулятором в интернете.
3. Рассчитать и изобразить эллиптические кривые с параметрами: b=1, a = 2 -3.
4. Написать программу сложения двух точек эллиптической кривой. Проверить алгоритм на графике.
5. Написать программу вычисления остатка от деления целого числа на заданный модуль для положительных и отрицательных чисел.
6. Написать программу поиска мультипликативной инверсии числа в поле Fp с и использованием расширенного алгоритма Эвклида.
7. Написать программу нахождения частного от деления двух целых чисел в модулярной арифметике.
8. Вычислить все точки, принадлежащие группе точек эллиптической кривой по модулю p<1000. Изобразить на графике.

9. Написать программу вычисления скалярного произведения точки на число методом удвоения – сложения.
10. Определить циклическую подгруппу, выбрав базовую точку из точек, принадлежащих некоторой группе на эллиптической кривой (см. задание 1).
11. Написать программу перекодировки произвольного длинного числа из 16-ричного формата (строки байтов) в формат Base58.
12. Написать программы раскодировки, т.е. перевода строки формата Base58 в 16-ричный формат.
13. Используя стандартные криптографические библиотеки написать программу получения электронной подписи и ее проверки.

Задания к разделу 2

1. Написать программу создания нового блока для криптовалюты, используя стандартные криптографические библиотеки. Промоделировать майнинг, создавая блоки с заданным условием на значение хеша.
2. Написать программу для создания транзакции.
3. Практическая работа в сети для учебной криптовалюты.

Задания к разделу 3

1. Получить последний блок на сайте «blockchain.info» , посмотреть структуру, значения констант сложность, nonce, количество нулей в хеше.
2. Получить транзакцию из этого блока (любую), посмотреть скрипты, расшифровать их.

8.1.3. Оценочные средства для промежуточной аттестации

Материалы для проведения текущего и промежуточного контроля знаний студентов:

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1.	Собеседование при защите готовой программы	Все темы	ПК-3
2.	Подготовка к зачету	Все разделы	ПК-3

Примерный список вопросов к зачёту:

- Блокчейн. Дайте определение. Каковы его свойства? Приведите примеры.
- Какие типы блокчейнов существуют?
- Что такое задача консенсуса?
- Какими свойствами обладает консенсус, основанный на доказательстве выполнения работы?

- Доказательство выполнения работы в сети Биткоин.
- Как устроен криптографический алгоритм с открытым ключом RSA?
- Сформулируйте задачу доказательства с нулевым разглашением.
- Как устроен алгоритм разделения секрета по схеме Шамира?
- Криптографические хэш функции.
- Задача консенсуса. Теорема FLP.

- Микроплатежи и умные контракты
- Какие возможности есть в языке Биткоин скрипт?
- Как устроены микроплатежи в Биткоине?

- Как устроен язык Солидити?

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

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

Пример тестовых заданий для проверки сформированности компетенций, указанных выше в п.III:

1. Приведены четыре дайджеста, полученных хешированием различных текстов методом SHA256. Какой из них ошибочный?

1) 6ed2cf20c6231a153fc3959fc10bbe8923f4bb9402cdbef7f1807a6b301b0437
2) 4ae7c3b6ac0beff671efa8cf57386151c06e58ca53a78d8uf36107316cec125f
3) c9c9df56e2529684f8742be7c27d9fc47c2ec708d50342297cc2e43faf90d822
4) 4afe0b28a14803a191c75e35a383e58d9e890dffe6a0e80277c5f2a244b1990c

2. Что является суммой двух точек на эллиптической кривой.

1) Точка, координаты которой равны сумме координат двух точек.
2) Точка, обратная точке, в которой эллиптическая кривая пересекается линией, соединяющей заданные две точки.
3) Точка, координаты которой равны разности координат двух точек.
4) Точка эллиптической кривой, образующая с первыми двумя равносторонний треугольник.

3. Что представляет собой приватный адрес?

1) Случайное 256- битное число.
2) Номер в списке пользователей блокчейна
3) Хеш фамилии пользователя.
4) Название группы пользователей блокчейна

4. Что такое майнинг?

1) Поиск спрятанных в сети денег.
2) Договор с пользователями блокчейна о распределении криптовалюты
3) Обслуживание пользователей блокчейна за определенный гонорар.
4) Создание нового блока, хеш которого меньше заданного числа.

5. Как обеспечивается надежная связь между блоками с данными в блокчейне?

1) Использование электронной подписи
2) Организация прав доступа пользователей
3) Добавление в состав блока хеша предыдущего блока
4) Шифрование информации

6. Что такое транзакции?

1) Состояние блокчейна на текущий момент
2) Записи о движении криптовалюты между кошельками
3) Переход от одного блока к другому в блокчейне
4) Запись в компьютере текущих действий с блокчейном

7. Приведены примеры, как можно заработать криптовалюту. Укажите ошибочное утверждение.

1) Создание нового блока в процессе майнинга
2) Поступление криптовалюты за счет перевода с других кошельков
3) Запись произвольной суммы в свой кошелек
4) Комиссионные за включение чужих транзакций в новый блок майнером

8. Пул транзакций – это

1) Список неподтвержденных транзакций для включения в новые блоки
2) Организация группы майнеров для совместной работы
3) Исчерпывающий список пользователей блокчейна
4) Максимальное количество возможных транзакций

Разработчики:

_____	доцент, к.ф.-м.н.	В.И., Красов
(подпись)	*(занимаемая должность)*	*(инициалы, фамилия)*

Программа рассмотрена на заседании кафедры общей и космической физики ИГУ
«__15__» _марта_ 2023__г.

Протокол № _8_, зав. кафедрой _____ В.Л. Паперный