

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЄРЕВАНСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**



З А Т В Е Р Д Ж У Ю
Директор Єреванського навчально-наукового
інституту ЗУНУ

Саша ГУДРАТЯН

2024 р.

З А Т В Е Р Д Ж У Ю
Проректор з науково-педагогічної роботи



Віктор ОСТРОВЕРХОВ

2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Блокчейн та децентралізовані системи» "

ступінь вищої освіти – бакалавр

галузь знань - 12 Інформаційні технології

спеціальність - 123 Комп'ютерна інженерія

освітньо-професійна програма- «Комп'ютерна інженерія»

Кафедра фундаментальних дисциплін

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)	Екз. (сем.)
Заочна	3	6	8	4	-	-	138	150	6	-

Єреван- ЄННІ ЗУНУ – 2024

Робочу програму розробив к.т.н., ст. викладач кафедри фундаментальних дисциплін ЄННІ
ЗУНУ Мурадян Армен



Робоча програма затверджена на засіданні кафедри фундаментальних
дисциплін, протокол № 1 від 27.08.2024 року.

Завідувач кафедри
фундаментальних дисциплін,
доктор технічних наук, професор



Гамлет АРУТЮНЯН

Розглянуто та схвалено групою забезпечення спеціальності 123
“Комп’ютерна інженерія”, протокол № 1 від 30.08.2024 р.

Голова ГЗС,
д.т.н., професор



Гамлет АРУТЮНЯН

Гарант
д.т.н., професор



Гамлет АРУТЮНЯН

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Блокчейн та децентралізовані системи»

Дисципліна «Блокчейн та децентралізовані системи»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 5	Галузь знань – 12 Інформаційні технології	Статус дисципліни вибіркова Мова навчання українська, вірменська
	Спеціальність – 123 Комп'ютерна інженерія	Рік підготовки: 3 Семестр: 6
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год): 8 Практичні заняття (год): 4
Загальна кількість годин – 150		Самостійна робота (год): 138
		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни «Блокчейн та децентралізовані системи»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Блокчейн та децентралізовані системи» є формування у студентів цілісного уявлення про суть технології блокчейн та переваги її використання в різних сферах діяльності людини.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни «Блокчейн та децентралізовані системи» отримання студентами теоретичних знань, спеціальних умінь і практичних навичок з використання технології блокчейн.

2.3. В результаті вивчення дисципліни студент повинен знати:

- принципи та переваги децентралізації;
- методи, алгоритми та програмні засоби забезпечення цілісності та конфіденційності даних в технології блокчейн;
- криптографію на основі еліптичної кривої;
- структуру даних Дерева Merkle;
- принцип функціонування блокчейн;
- алгоритми доказу виконаної роботи;
- принцип роботи та різновиди цифрових підписів;
- принципи роботи криптовалюти біткоїн;
- формати ключів у Bitcoin.

2.4. В результаті вивчення дисципліни студент повинен уміти:

- використовувати технологію блокчейн у професійній діяльності, оцінювати її ефективність;
- розробляти та впроваджувати інформаційні системи на основі технології блокчейн та цифрових валют;
- застосовувати різні типи платформ для розробки додатків на основі технології блокчейн.
- застосовувати алгоритми консенсус у децентралізованих системах..

3. Програма навчальної дисципліни: «Блокчейн та децентралізовані системи»

Змістовий модуль 1. Технології блокчейн.

Тема 1. Вступ до криптографії та криптовалют.

Криптографічні хеш-функції. Хеш-вказівники та структури даних. Цифрові підписи. Відкриті ключі як ідентичність. Проста криптовалюта.

Література: 1, 2.

Тема 2. Децентралізація та криптовалюта біткоїн.

Централізація проти децентралізації. Розподілений консенсус. Консенсус без ідентичності з використанням ланцюжка блоків. Стимули та доказ роботи.

Тема 3. Алгоритми доказу виконаної роботи.

PoW (Proof-of-work). PoS (Proof of Stake), DPOS (delegated Proof of Stake), Proof of Activity (PoW + PoS), Proof of Burn, Proof of Capacity, Proof-of-Storage, PoSe (proof-of-service).

Тема 4. Механізм біткоїнів.

Біткоїн-операції. Сценарії біткоїнів. Застосування скриптів біткоїн.

Біткоїн-блоки. Мережа біткоїнів. Обмеження та вдосконалення.

Тема 5. Як зберігати та використовувати біткоїни.

Просте локальне сховище. Гаряче та холодне зберігання. Розбиття та спільне використання ключів. Інтернет-гаманці та біржі. Платіжні послуги. Комісія за транзакції. Ринки валютних бірж.

Тема 6. Видобуток біткоїнів.

Завдання майнерів біткоїнів. Обладнання для майнінгу. Енергоспоживання та екологія. Гірничі стимули та стратегії.

Тема 7. Біткоїни та анонімність.

Основи анонімності. Як деанонізувати біткоїн. Змішування.

Децентралізоване змішування. Zerocoin і Zerocash.

Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти

Тема 8. Політика та регулювання.

Консенсус у біткоїнах. Основне програмне забезпечення Bitcoin. Зацікавлені сторони: Хто відповідає? Коріння біткоїна. Уряди звертають увагу на біткоїн. Заборона відмивання грошей.

Тема 9. Альтернативні обчислювальні задачі.

Основні вимоги до обчислювальних задач (головоломок). Стійкі до ASIC головоломки. Підтвердження корисної роботи. Головоломок, що не підлягають передачі. Доказ ставки та віртуальний майнінг.

Тема 10. Біткоїн як платформа.

Біткоін як журнал лише додатків. Біткоіни як "розумне майно". Захист багатосторонніх лотерей у біткоінах. Біткоін як публічне джерело випадковості. Ринки прогнозування та канали даних у реальному світі.

Тема 11. Альткоїни та екосистема криптовалют.

Альткоїни: історія та мотивація. Декілька деталей альткоїнів. Взаємозв'язок між біткоінами та альткойнами. Майнінг злиття. Альткойни з підтримкою біткоінів, "Бічні ланцюги". Ethereum та смарт-контракти

Тема 12. Децентралізовані системи: майбутнє біткоінів?

Ланцюг блоків як засіб для децентралізації. Шляхи до блокування ланцюгової інтеграції. Шаблон для децентралізації. Коли децентралізація є гарною ідеєю?

4. Структура залікового кредиту з дисципліни «Блокчейн та децентралізовані системи» (заочна форма навчання)

	Кількість годин		
	Лекції	Практичні заняття	СРС
Змістовий модуль 1. Технології блокчейн			
Тема 1. Криптографії та криптовалюти	2	2	8
Тема 2. Децентралізація та криптовалюта біткоін			10
Тема 3. Алгоритми доказу виконаної роботи			12
Тема 4. Механізм біткоінів	2		12
Тема 5. Як зберігати та використовувати біткоіни			12
Тема 6. Видобуток біткоінів			12
Тема 7. Біткоіни та анонімність			12
Змістовий модуль 2. Імітаційне моделювання та методи побудови й аналізу якості моделей			
Тема 8. Політика та регулювання	2	2	12
Тема 9. Альтернативні обчислювальні задачі			12
Тема 10. Біткоін як платформа			12
Тема 11. Альткоїни та екосистема криптовалют	2		12
Тема 12. Децентралізовані системи: майбутнє біткоінів.			12
Разом	8	4	138

5. Тематика практичних занять

Практичне заняття №1

Тема: Принципи роботи криптовалюти біткоін. Питання для обговорення:

1. Відправлення та отримання біткоінів
2. Звичайні форми транзакцій.

3. Конструкція транзакції.

Практичне заняття №2

Тема: Криптографія та криптовалюти.

Питання для обговорення:

1. Поняття хеш – функції.
2. Алгоритми обчислення хеш – функції.
3. Дослідження хеш – функції.
4. Алгоритми шифрування з відкритими ключами.
5. Алгоритми шифрування із закритими ключами.

Практичне заняття №3

Тема: Принципи технології

Blockchain Питання для

обговорення:

1. Структура блоку. Заголовок блоку. Блок генезису.
2. З'єднання блоків у Blockchain.
3. Дерево Меркле (Merkle).

Практичне заняття №4

Тема: Алгоритми доказу виконаної роботи

Питання для обговорення:

1. PoS (Proof of Stake),
2. DPoS (delegated Proof of Stake),
3. Proof of Activity (PoW + PoS),
4. Proof of Burn, Proof of Capacity, Proof-of-Storage, PoSe (proof-of-service)

Практичне заняття №5

Тема: Мережа Bitcoin

1. Питання для обговорення:
2. Архітектура однорангової мережі.
3. Типи вузлів і їх задачі.
4. Розширена мережа Bitcoin.

Практичне заняття №6

Тема: Проект Ethereum

Питання для обговорення:

1. Середовище розробки.
2. Мови програмування для платформи Ethereum (Serpent; Mutan; Solidity; LLL).
3. Ethereum – акаунти.
4. Повідомлення і транзакції.

5. Виконання коду. Блокчейн і майнінг.
6. Децентралізоване зберігання файлів.

Практичне заняття №7

Тема: Платформи для проектування додатків на основі технології блокчейн
Питання для обговорення:

1. Azure Blockchain Service Microsoft,
2. IBM Watson IoT.
3. Amazon Blockchain IoT.

6. Самостійна робота

Самостійне завдання студента полягає у виконанні наскрізного завдання «Розробка простого блокчейн-додатку».

Мета завдання. Ознайомити студентів з основами технології блокчейн, принципами її роботи, а також навчити їх розробляти прості додатки на основі блокчейн-технологій.

Завдання. Студенти повинні створити простий блокчейн-додаток, який реалізує функціонал зберігання та верифікації транзакцій. Додаток повинен включати наступні компоненти:

1. Структура блоку:
 - 1) ідентифікатор блоку (номер блоку);
 - 2) хеш попереднього блоку;
 - 3) час створення блоку;
 - 4) список транзакцій;
 - 5) чеш блоку.
2. Транзакції: створити просту структуру для транзакцій, яка включає:
 - 1) відправник;
 - 2) одержувач;
 - 3) сума;
 - 4) Час створення транзакції.
3. Основні функції:
 - 1) додавання нового блоку до блокчейну;
 - 2) верифікація цілісності блокчейну (перевірка хешу);
 - 3) виведення інформації про блокчейн (всі блоки та транзакції)ю

Технології: мова програмування: Python/JavaScript/Java (на вибір).

Бібліотеки:

- 1) для Python: Flask для створення API, hashlib для хешування;
- 2) для JavaScript: Express для створення API, crypto для хешування;
- 3) для Java: Spring Boot для створення API, java.security для хешування.

Кроки виконання:

1. Дослідження:
 - 1) ознайомитися з основами блокчейн-технології;

- 2) вивчити принципи роботи хеш-функцій та їх роль у блокчейні.

2. Розробка:

- 1) створити структуру блоку та транзакції;
- 2) реалізувати функцію додавання блоку до блокчейну;
- 3) реалізувати верифікацію блокчейну.

3. Тестування.

1. Провести тестування на коректність роботи додатку.
2. Перевірити, чи правильно відображаються дані про транзакції та блоки.

1. Презентація. Підготувати коротку презентацію (5-10 хвилин) про реалізований проект, описати обрані технології, алгоритми та результати тестування.

Критерії оцінювання:

- 1) коректність реалізації (40%);
- 2) якість коду (30%);
- 3) презентація (30%).

Термін виконання. Завдання має бути виконано та представлене до 15 навчального

тижня.

Рекомендації:

- 1) використовуйте Git для контролю версій вашого проекту.
- 2) досліджуйте існуючі блокчейн-проекти для натхнення.
- 3) пам'ятайте про безпеку даних при розробці.

7. Методи навчання.

У навчальному процесі застосовуються лекції в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, самостійна робота студентів, робота в Інтернет.

8. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Блокчейн та децентралізовані системи» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- оцінювання виконання лабораторних робіт;
- оцінювання результатів самостійної роботи.

9. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни «Блокчейн та децентралізовані системи» використовуються наступні методи оцінювання навчальної роботи студента:

- поточне тестування та опитування;

- оцінювання наскрізного проекту у результаті самостійної роботи;
- залік.

Оцінювання здійснюється за 100 бальною шкалою.

Критерії оцінювання знань:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без

аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань.

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	вілмінно	A
85–89	добре	B (дуже
75–84		C (добре)
65–74	задовільн о	D
60–64		E
35–59	незадовільн о	FX (незадовільно з можливістю повторного склання)
1–34		F (незадовільно з обов'язковим повторним

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер
1.	Мультимедійний	1 - 12
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. Освіти в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.
2. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
3. V.Yatskiv, N.Yatskiv, O. Bandrivskiy. “Proof of Video Integrity Based on Blockchain”, in *Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on*, 2019, pp. 431-434.
4. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security Internet of Things: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, Ternopil National Economic University, 2019. – 98 p.
5. Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 2.
6. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 p.
7. Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T., & Zhao, C. (2021). Blockchain-based efficient device authentication protocol for medical cyber-physical systems. *Security and Communication Networks*, Volume 2021, 2021, Article ID 5580939, 13 p. <https://doi.org/10.1155/2021/5580939>
8. Xu, J., Wang, C., & Jia, X. (2023). A survey of blockchain consensus protocols. *ACM Computing Surveys*, 55(13s), 1-35. <https://doi.org/10.1145/3579845>
9. Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain integration in the era of industrial metaverse. *Applied Sciences*, 13(3), 1353. <https://doi.org/10.3390/app13031353>
10. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3), 546. <https://doi.org/10.3390/electronics12030546>
11. Zhou, S., Li, K., Xiao, L., Cai, J., Liang, W., & Castiglione, A. (2023). A systematic review of consensus mechanisms in blockchain. *Mathematics*, 11(10), 2248. <https://doi.org/10.3390/math11102248>