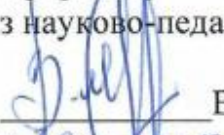


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
 ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
 ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**ЗАТВЕРДЖУЮ**  
 Декан факультету комп'ютерних  
 інформаційних технологій  
  
 Ігор ЯКИМЕНКО  
 «30» \_\_\_\_\_ 2024р.

**ЗАТВЕРДЖУЮ**  
 Проректор  
 з науково-педагогічної роботи  
  
 Віктор ОСТРОВЕРХОВ  
 «30» \_\_\_\_\_ 2024р.

**ЗАТВЕРДЖУЮ**  
 Директор навчально-наукового  
 Інституту новітніх освітніх технологій  
  
 Святослав ПИТЕЛЬ  
 \_\_\_\_\_ 2024р.



### РОБОЧА ПРОГРАМА

з дисципліни «Блокчейн та децентралізовані системи»  
 ступінь вищої освіти – бакалавр  
 галузь знань – 15 Автоматизація та приладобудування  
 спеціальність – 152 Метрологія та інформаційно-вимірювальна техніка  
 освітньо-професійна програма – Технології інтернету речей

#### Кафедра кібербезпеки

| Форма навчання | Курс | Семестр | Лекції (год.) | Практ. (семін.) (год.) | ІРС (год.) | Тренінг, (год.) | Самост. робота студ. (год.) | Разом (год.) | Залік (сем.) |
|----------------|------|---------|---------------|------------------------|------------|-----------------|-----------------------------|--------------|--------------|
| Денна          | 3    | 6       | 32            | 14                     | 3          | 6               | 95                          | 150          | 6            |
| Заочна         | 3    | 6       | 8             | 4                      |            |                 | 138                         | 150          | 6            |

Тернопіль – 2024

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26. 08. 2024 р.

Завідувач кафедри кібербезпеки



Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності протокол № 1 від 30,08. 2024 р.

Голова групи  
забезпечення спеціальності



Андрій СЕГІН

Гарант освітньо-професійної  
програми



Богдан МАСЛИЯК

## СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### 1. Опис дисципліни «Блокчейн та децентралізовані системи»

| Дисципліна<br>«Блокчейн та децентралізовані системи» | Галузь знань,<br>спеціальність, СВО  | Характеристика<br>навчальної дисципліни   |
|--|--|---|
| Кількість кредитів ECTS – 5                          | Галузь знань<br>Автоматизація та приладобудування  | <b>Статус дисципліни</b><br>вибіркова<br><br><b>Мова навчання</b><br>українська   |
| Кількість залікових модулів – 3                      | Спеціальність – 152 Метрорологія та інформаційно-вимірювальна техніка<br>Освітньо-професійна програма – Технології інтернету речей | Рік підготовки:<br><i>Денна – 3</i><br><br>Семестр:<br><i>Денна – 6</i>   |
| Кількість змістових модулів – 2                      | Ступінь вищої освіти – бакалавр  | Лекції (год):<br><i>Денна – 32</i><br><i>Заочна – 8</i><br>Практичні заняття (год):<br><i>Денна – 14</i>                            |
| Загальна кількість годин – 150                       |  | Самостійна робота (год):<br><i>Денна – 95</i><br><i>Тренінг (год): денна – 6</i><br>Індивідуальна робота (год):<br><i>Денна – 3</i> |
| Тижневих годин – 10,<br>з них аудиторних – 3         |  | 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 консенсусу 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.

Література: 1, 2.

#### **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).

Література: 1, 3, 5.

**Тема 4.** Механізм біткоїнів.

Біткоїн-операції. Сценарії біткоїнів. Застосування скриптів біткоїнів. Біткоїн-блоки. Мережа біткоїнів. Обмеження та вдосконалення.

Література: 2, 3, 6

**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.

Література: 1, 2, 3.

**Тема 6.** Видобуток біткоїнів.

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

Література: 1, 2, 4,

**Тема 7.** Біткоїни та анонімність.

Основи анонімності. Як деанонімізувати біткоїн. Змішування. Децентралізоване змішування. Zerocoin і Zerocash.

Література: 1, 2, 5,

**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.

Література: 2, 3, 9.

**Тема 9.** Альтернативні обчислювальні задачі.

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

Література: 2, 3, 10

**Тема 10.** Біткоїн як платформа.

Біткоїн як журнал лише додатків. Біткоїни як "розумне майно". Захист багатосторонніх лотерей у біткоїнах. Біткоїн як публічне джерело випадковості. Ринки прогнозування та канали даних у реальному світі.

Література: 2, 3, 4, 10.

**Тема 11.** Альткоїни та екосистема криптовалют.

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

Література: 1, 2, 4.

**Тема 12.** Децентралізовані системи: майбутнє біткоїнів?

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

Література: 1, 2, 5, 10.

**4. Структура залікового кредиту  
з дисципліни «Блокчейн та децентралізовані системи»**

**денна форма навчання**

|  | Кількість годин |                   |           |          |          |                    |
|--|-----------------|-------------------|-----------|----------|----------|--------------------|
|  | Лекції          | Практичні заняття | СРС       | ІРС      | Тренінг  | Контрольні заходи  |
| <b>Змістовий модуль 1. Технології блокчейн</b>                                 |                 |                   |           |          |          |                    |
| Тема 1. Криптографії та криптовалюти   | 2               |                   | 7         | 1        | 3        | Поточне опитування |
| Тема 2. Децентралізація та криптовалюта біткоін                                | 2               |                   | 8         |          |          |                    |
| Тема 3. Алгоритми доказу виконаної роботи                                      | 4               | 2                 | 8         |          |          |                    |
| Тема 4. Механізм біткоінів   | 4               | 2                 | 8         |          |          |                    |
| Тема 5. Як зберігати та використовувати біткоіни                               | 4               | 2                 | 8         |          |          |                    |
| Тема 6. Видобуток біткоінів  | 2               | 2                 | 8         |          |          |                    |
| Тема 7. Біткоіни та анонімність  | 2               |                   | 8         |          |          |                    |
| <b>Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти</b> |                 |                   |           |          |          |                    |
| Тема 8. Політика та регулювання  | 2               |                   | 8         | 2        | 3        | Поточне опитування |
| Тема 9. Альтернативні обчислювальні задачі                                     | 2               | 2                 | 8         |          |          |                    |
| Тема 10. Біткоін як платформа  | 2               | 2                 | 8         |          |          |                    |
| Тема 11. Альткоіни та екосистема криптовалют                                   | 4               | 2                 | 8         |          |          |                    |
| Тема 12. Децентралізовані системи: майбутнє біткоінів.                         | 2               |                   | 8         |          |          |                    |
| <b>Разом</b>   | <b>32</b>       | <b>14</b>         | <b>95</b> | <b>3</b> | <b>6</b> |                    |

**заочна форма навчання**

|  | Лекції   | Практичні заняття | СРС        |
|--|----------|-------------------|------------|
| Тема 1. Криптографії та криптовалюти                   | 2        | 1                 | 10         |
| Тема 2. Децентралізація та криптовалюта біткоін        |          |                   | 14         |
| Тема 3. Алгоритми доказу виконаної роботи              |          |                   | 10         |
| Тема 4. Механізм біткоінів                             | 2        | 1                 | 15         |
| Тема 5. Як зберігати та використовувати біткоіни       |          |                   | 10         |
| Тема 6. Видобуток біткоінів                            |          |                   | 10         |
| Тема 7. Біткоіни та анонімність                        | 2        | 1                 | 10         |
| Тема 8. Політика та регулювання                        |          |                   | 15         |
| Тема 9. Альтернативні обчислювальні задачі             |          |                   | 10         |
| Тема 10. Біткоін як платформа                          | 2        | 1                 | 14         |
| Тема 11. Альткоіни та екосистема криптовалют           |          |                   | 10         |
| Тема 12. Децентралізовані системи: майбутнє біткоінів. |          |                   | 10         |
| <b>Разом</b>   | <b>8</b> | <b>4</b>          | <b>138</b> |

**5. Тематика практичних занять**

**Практичне заняття №1**

Тема: *Принципи роботи криптовалюти біткоін.*

Питання для обговорення:

1. Відправлення та отримання біткоїнів
2. Звичайні форми транзакцій.
3. Конструкція транзакції.

Література: 2, 3, 10.

### **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.

Література: 3, 12.

### **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).

Література: 1, 2, 5.

### **Практичне заняття №4**

Тема: Алгоритми доказу виконаної роботи для обговорення

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)

Література: 4, 5.

### **Практичне заняття №5**

Тема: Мережа Bitcoin

Питання для обговорення:

1. Архітектура однорангової мережі.
2. Типи вузлів і їх задачі.
3. Розширена мережа Bitcoin.

Література: 2, 3.

### **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.

Література: 4, 5.

## 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.

Література: 3, 4.

### 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) хеш 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)

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 представлено 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. Організація та проведення тренінгу з дисципліни «Блокчейн та децентралізовані системи»

| № п/п | Вид роботи           | Порядок проведення тренінгу   |
|-------|----------------------|---|
| 1     | Реалізація блокчейну | 1. Створення прототипу<br>2. Реалізація алгоритму Proof-of-Work<br>3. Постійна пам'ять та інтерфейс командного рядка<br>4. Транзакції<br>5. Адреси<br>6. Мережа |
| 2     | Запуск блокчейну     | Тестування та дослідження роботи блокчейну.<br>Область застосування та шляхи удосконалення блокчейну.   |

## 8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проєктора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

## 9. 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;
- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи.

## 10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Блокчейн та децентралізовані системи» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для заліку

| Модуль 1  |   | Модуль 2   | Модуль 3   |
|---|---|--|--|
| 40%   | 40%   | 5%   | 15%  |
| Поточне оцінювання  | Модульний контроль                              | Тренінги   | Самостійна робота  |
| Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-7. | Підсумкове модульне тестування за темами №1-12. | Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу. | Визначається як оцінка за наскрізне завдання самостійної роботи. |

Шкала оцінювання:

| За шкалою ЗУНУ | За національною шкалою | За шкалою ECTS |
|----------------|------------------------|----------------|
| 90–100         | відмінно               | A (відмінно)   |

|       |              |   |
|-------|--------------|---|
| 85–89 | добре        | В (дуже добре)                                      |
| 75-84 |              | С (добре)   |
| 65-74 | задовільно   | Д (задовільно)                                      |
| 60-64 |              | Е (достатньо)                                       |
| 35-59 | незадовільно | FX (незадовільно з можливістю повторного складання) |
| 1-34  |              | F (незадовільно з обов'язковим повторним курсом)    |

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

| №  | Найменування                                  | Номер теми |
|----|---|------------|
| 1. | Мультимедійний проєктор                       | 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. Bandrivskiyi. “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. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 p.
6. 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>
7. 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>
8. 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>
9. 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>
10. 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>