МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи
_____ Каріна НЕМАШКАЛО

БЛОКЧЕЙН: ОСНОВИ ТА ПРИКЛАДИ ВИКОРИСТАННЯ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**всі**
Спеціальність	**всі**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**всі**
Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Розробник: підписано КЕП
к.т.н., доц. Наталія ДОЛГОВА

Завідувач кафедри
кібербезпеки та
інформаційних технологій
д.т.н., проф. Ольга СТАРКОВА

Харків
2023

ВСТУП

Актуальність навчальної дисципліни “Блокчейн: основи та приклади використання” та її необхідність та роль у підготовці фахівців полягає у тому, що блокчейн є новітньою технологією, інтерес до якої зріс разом з популярністю криптовалют. Але є десятки інших способів використання блокчейна у відриві від криптовалюти. Блокчейн-технологію відносять до головного технологічного прориву з часів винаходу Інтернету.

Дисципліна “Блокчейн: основи та приклади використання” є навчальною дисципліною вільного вибору (вільний магмайнор) за усіма спеціальностями.

Метою викладання дисципліни є формування у здобувачів комплексного розуміння блокчейну як технології, його ключових аспектів і способів застосування в економічних і бізнес-контекстах.

Завданнями навчальної дисципліни включають у себе:

- розуміння основних принципів і механізмів роботи блокчейна,
- вивчення різних способів його застосування в економіці та бізнесі,
- розвиток навичок створення блокчейн-рішень для реальних бізнес-завдань.

Предметом дисципліни є дослідження блокчейн-технології, включно з її основами, такими як криптографія, консенсусні алгоритми, смарт-контракти та децентралізовані додатки. Крім того, до предмета входить аналіз способів застосування блокчейна в різних секторах економіки, включно з фінансами, логістикою, управлінням ланцюжками поставок тощо.

Об'єктом вивчення є блокчейн-системи і технології, а також їхнє практичне застосування в багатьох сферах діяльності. Це включає в себе різні типи блокчейнів (публічні, приватні, консорціумні), криптовалюти та їхнє функціонування, методи й інструменти розроблення та впровадження блокчейн-проектів у бізнес-процеси.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Компетентності та результати навчання за дисципліною

Результати навчання	Компетентності, якими повинен оволодіти здобувач вищої освіти
Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів.	Здатність обґрунтовувати економічні рішення на основі розуміння закономірностей економічних систем і процесів та із застосуванням сучасного методичного інструментарію.

	Здатність ефективно застосовувати інформаційні технології в бізнесі та управлінні фінансами.
Застосовувати набуті теоретичні знання для розв'язання практичних завдань та змістовно інтерпретувати отримані результати.	Здатність застосовувати комп'ютерні технології та програмне забезпечення з обробки даних для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Основи блокчейн технологій

Тема 1. Децентралізація в інформаційних системах

1.1 Визначення децентралізації?

Поняття децентралізації для інформаційних систем. Відмінність децентралізованих систем від систем із резервуванням

1.2 Історія децентралізованих систем

Децентралізовані файлообмінні системи. Децентралізовані системи передачі даних. Децентралізовані обчислювальні системи. Децентралізовані системи зберігання даних. Децентралізовані системи прийняття рішень. Децентралізовані платіжні системи

1.3 Застосування принципів децентралізації.

Обмеження та проблеми централізованих систем. Застосування децентралізованого підходу. Принципи побудови децентралізованих систем. Типова архітектура децентралізованих систем. Обмеження децентралізованих систем. Фактори, що уповільнюють впровадження децентралізованих систем.

Тема 2. Технологія блокчейн

2.1. Технологія блокчейн та її можливості

Ступені децентралізації . Архітектура blockchain. Властивості блокчейна. Застосування технології.

2.2 Відмінності підходів до досягнення консенсусу

Механізм досягнення консенсусу як ключовий елемент децентралізованої системи обліку. Proof-of-work. Proof-of-stake. Delegated proof-of-stake. Proof-of-importance. Основні критерії класифікації механізмів досягнення консенсусу.

2.3 Обмеження технології блокчейн і складнощі її застосування

Упровадження digital identity. Дигіталізація всіх процесів. Прийняття єдиних правил обробки даних Перенесення всіх цифрових активів до однієї облікової системи Організація децентралізованого прийняття рішень. Обмеження пропускної здатності. Обмеження часу підтвердження транзакції . Проблема управління (governance) Розподілена відповідальність. Проблема оновлення протоколу

Тема 3. Принцип роботи Bitcoin

3.1 Історія виникнення Bitcoin

Проблеми, які здатний вирішити Bitcoin. Головні принципи функціонування Bitcoin. Емісія в Bitcoin. Формування ціни на монети. Поняття довіри в Bitcoin. Обмеження технології Bitcoin. Значення децентралізації для Bitcoin.

3.2 Застосовування Bitcoin.

Ключі у Bitcoin. Транзакції в Bitcoin. Програмні гаманці. Апаратні гаманці. Централізовані сховища. Резервне копіювання гаманців

3.3 Поняття транзакції у Bitcoin.

Bitcoin-транзакція. Перевірка транзакцій. Поняття комісії у Bitcoin. Поняття конфліктуючих транзакцій.

3.4 Високорівнева архітектура Bitcoin.

Архітектура системи з технологією blockchain. Процеси в обліковій системі Bitcoin. Ролі учасників в обліковій системі Bitcoin. Умови, за яких досягається консенсус у Bitcoin. Консенсус в Bitcoin. Порівняння Bitcoin з традиційними платіжними системами

3.5 Підтвердження транзакцій у Bitcoin

Формування блоків транзакцій. Вимоги до нових блоків. Принципи змагання між користувачами. Розповсюдження блоку. Вирішення розбіжностей. Поняття повного підтвердження транзакції. Винагороди за створення блоків

Тема 4. Криптографії та управління ключами

4.1 Вступ до криптографії.

Принципи криптографічного захисту інформації. Поняття ключів. Модель загроз та порушника. Генерація та обробка секретних ключів. Поняття однонаправленої функції та NP-повної задачі. Геш-функція. Застосування геш-функцій. Дерева Меркла. Симетричне шифрування. Асиметрична криптографія.

4.2 Криптографія у Bitcoin

Особливості роботи еліптичних кривих. Створення Bitcoin-адрес. Конфіденційність в Bitcoin

4.3 Зберігання й обробка ключів

Головна задача цифрового гаманця. Основні підходи до синхронізації гаманця. Обробка та зберігання ключів на сервері. Ключі на сервері, але доступ до них тільки у клієнта. Ключі на пристрої користувача. Зберігання монет із застосуванням мультипідпису. Холодні, теплі та гарячі гаманці.

Змістовий модуль 2. Приклади застосування блокчейн технологій

Тема 5. Правила формування блоків в блокчейн

5.1. Реалізація блокчейн у Bitcoin

Структура блоку. Приклади блоків у Bitcoin. Ланцюжки блоків.

5.2. Поняття Mempool у Bitcoin

Життєвий цикл блоку. Початкова синхронізація вузла. Checkpoints. Властивості спільної бази даних Bitcoin

Тема 6. Правила роботи блокчейн в Bitcoin

6.1.Майнінг у Bitcoin

Поняття і цілі майнінгу в Bitcoin. Класифікація вузлів мережі. Поняття ресурсномісткого завдання. Обмеження частоти формування блоків. Orphan blocks. Атака подвійної витрати

6.2. Технічне забезпечення майнингу.

Поява та класифікація спеціального обладнання для майнингу. Майнінгові пули та їх завдання. Статистика майнингу і оцінка енергоспоживання.

Тема 7. Проведення транзакцій та формати ключів в Bitcoin

7.1 Транзакції в Bitcoin.

Структура транзакції. Unspent Transaction Outputs (UTXOs). Отримання решти та встановлення комісії. Схема передачі монет на прикладі. Формування транзакцій у bitcoin-гаманцях. Механізм LockTime. Off-chain протоколи. Signature hash types. Запис довільних даних до ланцюга блоків.

7.2. Механізм комісій у Bitcoin.

Волатильність ціни запису даних. Рішення проблеми з волатильністю комісій. Підвищення комісії після відправки транзакції. Segregated Witness та комісії. Варіант із другом-майнером. Варіант із продажом місць у черзі на підтвердження.

7.3. Особливості оновлення Segregated Witness

Збільшення пропускної здатності та зворотна сумісність. Нововведення Segregated Witness. Приклад SegWit-транзакції. Нові поняття ваги і розміру транзакції.

Тема 8. Блокчейн, криптовалюти та смарт-контракти

8.1 Відгалуження та клони Bitcoin

Спланові форки. Методи оновлення програмного забезпечення: softfork і hardfork. Незапланований softfork у Bitcoin. Поняття спланованих форків. Приклади спланованих форків Bitcoin.

8.2 Альтернативні цифрові валюти та токени.

Криптовалюті. Litecoin Dash. Відмінність алгоритмів майнінгу Litecoin, Dash і Bitcoin. BitShares. Monero . Ethereum. Cardano. Інші цифрові валюти. Токени.

8.3 Вступ до смарт-контрактів.

Визначення смарт-контракту. Роль оракулів для смарт-контрактів. Приклад із купівлею в онлайн-магазині. Приклад контракту для спільної купівлі. Класифікація платформ смарт-контрактів. Відмінність платформ за середовищем виконання. Відмінність платформ за способом виконання контрактів. Відмінність платформ за способом ініціювання контрактів.

Перелік лабораторних та практичних занять /завдань за навчальною дисципліною наведено в табл. 2.

Таблиця 2

Перелік лабораторних та практичних занять / завдань

Назва теми та / або завдання	Зміст
Тема 1. Завдання 1.	Дослідження алгоритмів хешування та їх використання в блокчейн
Тема 2. Завдання 2.	Робота з Metamask
Тема 3. Завдання 3.	Робота з паролями та геш-значеннями
Тема 4. Завдання 4.	Дослідження S-блоку та P-блоку
Тема 5. Завдання 5.	Робота з децентралізованим сховищем даних IPFS
Теми 6 – 7. Завдання 6.	Знайомство з процесом майнінгу та роботи з криптовалютою
Тема 8. Завдання 7.	Створення смарт-контрактів Ethereum

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3.

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1 - 8	Вивчення нового матеріалу: перегляд відео-лекцій та ознайомлення
Тема 1 -8	з технологією Блокчейн
Тема 1 -8	Поглиблене вивчення матеріалу: виконання типових задач

Кількість годин лекційних, та лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:

Словесні (лекція-візуалізація (Тема 1, 2, 3, 5, 6, 7, 8), лекція-семінар (Тема 4).

Наочні (демонстрація (Тема 1-8)).

Практичні (лабораторна робота (Тема 1 – 8)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних та лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів, а саме, для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формі семестрового заліку. Підсумкова оцінка за навчальною дисципліною з формою семестрового контролю залік визначається: сумуванням всіх балів, отриманих під час поточного контролю. Під час викладання навчальної дисципліни використовуються наступні контрольні заходи (поточний контроль):

виконання та захист лабораторних робіт (7 робіт по 10 балів кожна),

письмові контрольні роботи (3 роботи по 10 балів кожна).

Семестровий контроль: Залік.

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с.
2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.
3. Молчанов В. П. Технології розробки WEB-ресурсів [Електронний ресурс] : навч. посіб. / В. П. Молчанов, О. К. Пандорін ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (7,94 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 129 http://www.repository.hneu.edu.ua/handle/123456789/22466
4. Інформатика в сфері комунікацій [Електронний ресурс] : навч.-практ. посіб. : у 3-х ч. Ч. 3 : Використання web-технологій у сфері комунікацій / С. Г. Удовенко, В. А. Затхей, О. В. Гороховатський [та ін.] ; за заг. ред. С. Г. Удовенка; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (10.5 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. - 154 с. : іл. - Загол. з титул. екрану. - Бібліогр.: с. 153 http://repository.hneu.edu.ua/handle/123456789/24506

Додаткова

5.Global Bitcoin Nodes Distribution [Електронний ресурс]. – December 2018. – Режим доступу: https://bitnodes.earn.com/.
6. Накамото С. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoci Накамото. URL: https://bitcoin.org/bitcoin.pdf
7. Synergy of building cybersecurity systems: monograph / Edited by S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://repository.hneu.edu.ua/handle/123456789/25623
8. Розвиток блокчейн-бізнесу сприятиме економічному відновленню України // http://www.fin.org.ua/news/1452566[Електронний ресурс].
9. UA Крипта в Україні 2021 — гравці, закони, тенденції. URL: https://nachasi.com/crypto/2021/05/31/cryptotrends-in-ukraine/[Електронний ресурс].
10. Shmatko O. Information support for distributed teamwork knowledge management / O. Shmatko, M. Bilova. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– P. 169–192.http://repository.hneu.edu.ua/handle/123456789/24818

Інформаційні ресурси.

11. Сайт Distributed Lab // Blockchain Experts [Електронний ресурс]. – Режим доступу: https://distributedlab.com/
12. Blockchain Explorer–Search the Blockchain | BTC | ETH [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/explorer.
13. Сайт BlockchainDemo [Електронний ресурс]. – Режим доступу: https://blockchaindemo.io/