

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

Факультет інформаційних технологій

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС
з дисципліни

«Основи технології блокчейн»

для підготовки фахівців

Галузь знань **05 «Соціальні та поведінкові науки»**

Спеціальність **051 «Економіка»**

Освітня програма **«Цифрова економіка»**

Ступінь вищої освіти – Бакалавр

Київ – 2022 р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Декан факультету інформаційних технологій

_____ О.Г. Глазунова
(Підпис)

“25” травня 2022 р.

СХВАЛЕНО

на засіданні кафедри
інформаційних систем і технологій
Протокол № 9 від “ 15 ” квітня 2022 р.

Завідувач кафедри

_____ М.З. Швиденко
(Підпис)

РОЗГЛЯНУТО

Гарант ОП «Цифрова економіка»

_____ Н.А. Клименко
(Підпис)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи технології блокчейн»

Галузь знань **05 «Соціальні та поведінкові науки»**

Спеціальність **051 «Економіка»**

Освітня програма **«Цифрова економіка»**

Факультет інформаційних технологій

Розробники: к.е.н., доц. Швиденко М.З., к.е.н., доц. Рогоза К.Г.

Київ – 2022 р.

1. Опис навчальної дисципліни

«Основи технології блокчейн»

Галузь знань, напрям підготовки, спеціальність, ступень вищої освіти	
Ступень вищої освіти	<i>бакалавр</i>
Галузь знань	05 Соціальні та поведінкові науки
Спеціальність	051 Економіка
Освітньо-кваліфікаційна програма	Економічна кібернетика Цифрова економіка
Характеристика навчальної дисципліни	
Вид	Вибіркова
Загальна кількість годин	150
Кількість кредитів ECTS	5
Кількість змістовних модулів	2
Курсовий проект (робота) (за наявності)	-
Форма контролю	Екзамен
Показники навчальної дисципліни	
Форма навчання	<i>Денна</i>
Рік підготовки	<i>4</i>
Семестр	<i>8</i>
Лекційні заняття	<i>24</i>
Практичні, семінарські заняття	
Лабораторні заняття	<i>24</i>
Самостійна робота студента	<i>102</i>
Індивідуальні завдання	
Кількість тижневих аудиторних годин для денної форми навчання	<i>4 годин на тиждень</i>

2. Мета та завдання навчальної дисципліни

Дисципліна "Основи технології блокчейн" належить до спеціальних дисциплін, які забезпечують формування знань та навиків студентів з впровадження комп'ютерних технологій, зокрема, основ технології блокчейн у соціальних, технологічних, економічних та управлінських процесах.

Мета: сформувати у студентів систему знань в області основ технології блокчейн та її застосування в бізнес-процесах.

Завданнями курсу є:

- визначити теоретичні та економічні аспекти функціонування технології блокчейн та криптовалют;
- ознайомитися із механізмами блокчейн технологій;
- проаналізувати організаційні та методологічні основи технології блокчейн;
- ознайомитися з процедурою ICO;
- набути знань з питань майнінгу криптовалют;
- визначення основних сфер використання технології блокчейн;
- вивчити проблеми і перспективи розвитку технології блокчейн.

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- принципи та механізм технології блокчейн, основні етапи ICO, основні форми та методи майнінгу криптовалют;
- основи побудови блокчейн технології, принципи побудови, проведення та затвердження транзакцій криптовалют,
- принципи побудови і функціонування розумних контрактів, характеристику віртуальних грошей;
- основні можливості мови програмування Solidity.

уміти:

- налаштовувати оточення для створення приватного блокчейну;
- розробляти та удосконалювати смарт-контракти;
- створювати середовище та запускати ICO;

Набуття компетентностей:

загальні компетентності (ЗК):

- ЗК7. Навички використання інформаційних і комунікаційних технологій.
- ЗК8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- ЗК11. Здатність приймати обґрунтовані рішення.

фахові (спеціальні) компетентності (СК):

СК7. Здатність застосовувати комп'ютерні технології та програмне забезпечення з обробки даних для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів.

СК15. Уміння використовувати сучасні технології, інтелектуальні методи, цифрові та програмні інструменти з обробки й аналізу даних.

СК20. Здатність до роботи з сучасними системами та інструментами захисту цілісності та доступності економічної інформації

Програмні результати, а саме:

ПРН12. Застосовувати набуті теоретичні знання для розв'язання практичних завдань та змістовно інтерпретувати отримані результати.

ПРН 19. Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів.

3.Програма та структура навчальної дисципліни

Змістовий модуль 1. Складові технології блокчейн

Тема 1. Введення до технології блокчейн

Історія виникнення і розвитку Bitcoin. Ключові особливості Bitcoin: вся система децентралізована, севдоанонімність, незворотність, безпека, прямий характер операцій. Принципи роботи Bitcoin архітектури. Блокчейн біткоіна – розподілена база даних. Як влаштований блокчейн Bitcoin – нововведення: P2P мережі, хешування і асиметрична криптографія, в)розподілений консенсус, заснований на вирішенні трудомісткої математичної задач. Криптографічні механізми в Bitcoin. Криптографічно стійкі хеш-функцій, застосовувані в криптографії: незворотність, стійкість колізіям першого роду, стійкість до колізій другого роду. Генератор хеш-функцій FILEFORMAT.INFO. Аасимеричні методи шифрування. Відкритий(public) та закритий(private) ключі шифрування. Поняття консенсусу. Proof-of-Work (PoW – підтвердження роботи) – алгоритм захисту розподілених систем від зловживань (DoS-атак, спам-розсилок і т.д.). Як функціонує блокчейн. Формування блоків. Блоки в блокчейні і їх зв'язок між собою. Вміст заголовка блоку. Суть дерева Меркла (Merkle tree) – бінарне дерево хешів. Власне вміст (Payload) блоку. Реалізація протоколу Proof-of-Work – доказу роботи. Поняття майнінгу. Параметр nonce. Повні та легкі ноди. Кількість повних нод блокчейну.

Тема 2. Як функціонує блокчейн.

Визначення Ефіріума. Ethereum (ефіріум, ефір) – криптовалюта і функціональне децентралізована середовище. Історія створення Ефіріума. Краудфандінг. ICO Ethereum. The

DAO-платформа для пошуку проектів для інвестування, побудованих на смарт-контрактах. ICO The DAO- найуспішніше в історії за збором коштів. Хардфорк Ethereum – Ethereum Classic – версія «до відкату». Запуск Ethereum змінює весь криптовалютний світ. Платформа Ethereum-середовище для розробки і функціонування децентралізованих додатків на базі blockchain з використанням smart-контрактів сприймає будь-яку мову програмування, включаючи мови візуального програмування. Універсальність і гнучкість платформи Ethereum. Віртуальна машина Ethereum (EVM). Основні відмінності Ефіріума і біткоіну. Поняття смарт-контракту. Ключові переваги та деякі недоліки смарт-контрактів. Визначення смарт-контракту. Принципи роботи смарт контрактів. Класифікація смарт-контрактів. Смарт-контракти за середовищем виконання. Смарт-контракти за способом завдання та виконання умов. Смарт-контракти за способом ініціації. Функціонування блокчейну Ethereum. Користувальницький аккаунт. Види вузлів. Транзакції. Газ в смарт-контрактах. Особливості майнінгу в Ефіріумі.

Тема 3. Токенізація та ICO

Сутність ICO (Initial Coin Offering - «первинне розміщення монет»). ICO – це відносно нова форма інвестування, поява якої пов'язано зі становленням криптовалют. Відмінність ICO від традиційного збору коштів. Основні етапи ICO. Pre-ICO або Pre-Sale – це залучення інвестицій ще до початку самого ICO. Краудсейл (CrowdSale) – основний етап продажу монет, тобто, сам ICO. Продажі токенив на внутрішньому рівні – через платформу (сайт) стартапа, або на криптовалютних біржах. Баунті (Bounty) – винагорода, пропоноване ініціаторам ICO за певні послуги. White Paper (біла книга) – опис ICO-детальне розкриття суті ідеї, опис методів її реалізації – розкриваються технічні, маркетингові деталі стартапу. Roadmap (дорожня карта, карта розвитку) – хронологія розвитку проекту. Юрисдикція – країна, де зареєстровано юридичну особу, що ініціювала ICO. Скам – шахрайський проект, метою якого є залучення коштів шляхом ICO без подальшого розвитку своєї ідеї. Приклади крупних ICO. Поняття токенив. Види токенив. Equity tokens – являють собою акції компанії. Utility tokens – відображають деяку цінність в рамках бізнес-моделі онлайн-платформи (репутація, бали за певні дії, ігрова валюта). Asset-backed tokens – цифрові зобов'язання на реальні товари або послуги.

Тема 4. Розвиток технології блокчейн

«Альткоіни»-«альтернативні біткоіну монети». Причини виникнення альткоінів. Види альткоінів. Найбільш поширені альткоіни. Дорожня карта Ефіріума. Ethereum 1.0. Frontier (Липень 2015): Перший реліз мережі Ethereum. Homestead (Березень 2016): виробничий випуск. EIP(пропозицій щодо поліпшення Ethereum). Byzantium (Жовтень 2017): Metropolis: швидше і безпечніше. 3 релізи: Constantinople (Лютий 2019). Istanbul (грудень 2019). Ethereum 2.0 – Serenity – фінальний етап розвитку Ефіріума – Ефіріум 2.0- зміна консенсусу PoW на PoS, гнучка і

масштабована мережа, повнофункціональне розподілене програмне забезпечення. Casper – оновлення мережі Ethereum, яке передбачає перемикавання алгоритму на Proof of Stake (PoS) (також відоме як Ethereum 2.0). Переваги та недоліки Casper. Технологія шардінгу (sharding). Особливості, переваги та проблемні питання застосування технології шардінгу. Розвиток протоколів досягнення консенсусу. Модифікації PoW-протоколів: SPECTRE і PHANTOM. Опис та принципи реалізації протоколу Proof-of-Stake (PoS – Доказ частки). Delegated Proof-of-Stake (DPoS) (Делегований доказ частки). Byzantine Fault Tolerance (BFT) протоколи. Practical Byzantine Fault Tolerance (PBFT) (Реалізація протоколу завдання візантійських генералів). Delegated Byzantine Fault Tolerance (DBFT) (Делегований протокол завдання візантійських генералів). *Приклади BFT-протоколів*. Модифіковані протоколи консенсусу: Proof-of-Activity (PoA) (*Доказ активності*). Proof-of-Location (PoL) (*Доказ розташування*) Proof-of-Importance (PoI) (*Доказ важливості*) та інші.

Змістовий модуль 2. Прикладні аспекти технології блокчейн

Тема 5. Приватні блокчейни

Визначення приватного блокчейну. Публічний блокчейн (public blockchain), в якому транзакції відбуваються у вільному порядку і ніким не контролюються. Блокчейн, що належить консорціуму (consortium blockchains) - в ньому транзакції узгоджуються відібраними консорціумом вузлами. Приватна мережа (fully private blockchain) – в ній присутній центральний орган, який і контролює всі транзакції. Unpermissioned public ledgers або публічні реєстри відкритого типу; permissioned public ledgers або публічні реєстри закритого типу; permissioned private ledgers – приватні реєстри з закритим доступом. Рівні управління блокчейнами. Публічні децентралізовані системи. Громадські організації з делегованим управлінням. Приватні контрольовані блокчейни. Особливості, характеристика, алгоритм консенсусу та принципи функціонування платформи Echonum. Блокчейн як послуга (Blockchain-as-a-Service). Компанії провайдери послуги Blockchain-as-a-Service. Hyperledger – проект з відкритим вихідним кодом Linux Foundation. Архітектура проектування Hyperledger: модульна конструкція, повністю безпечна платформа, функціональна сумісність, криптовалюта-агностик, підтримка високого класу API. Інструменти Hyperledger-Caliper, Hyperledger-Cello, Hyperledger-Composer, Hyperledger-Explorer, Hyperledger-Quilt, Hyperledger-Ursa. Порівняння Hyperledger та Ethereum. Hyperledger Fabric- основні характеристики та принципи роботи.

Тема 6. Децентралізовані додатки (DApps)

Визначення DApps (decentralized applications). Критерії, яким повинні відповідати DApps. Фронтенд (frontend) і бекенд (backend) централізованих додатків та їх відмінності від звичайних додатків. Переваги DApps. Стабільність роботи. Прозорість. Класифікація DApps. Тип 1 –

додатки, які працюють на своєму власному блокчейне. Тип 2 – додатки, які розроблені і працюють на основі вже існуючого блокчейна. Тип 3 – додатки, засновані на додатках, заснованих на блокчейні. Децентралізовані фінанси (DeFi). Основні переваги DeFi. Різниця між DeFi і Open Banking. Платформи Dapps: Ethereum, EOS, TRON, NEO. Області застосування Dapps. Аукціони. Ринки пророкувань. Ідентифікація користувачів. Геймінг і гемблінг. Децентралізовані стейблкоїни. Некастодіальні лендінгові протоколи. Децентралізовані біржі (DEX). Однорангові ринки передбачень. Синтетичні активи. Платформи з випуску токенизованих цінних паперів (Security Token Offering). Управління активами. DeFi-ескроу. Недоліки і ризики DeFi. Системні ризики. Ризик злому смарт-контрактів. Централізація потоку даних. Недолік капіталу в DeFi-позиках.

Тема 7. Застосування технології блокчейн

Сфери використання блокчейну. Цифрові активи і токенизація. Торгівля. Логістика. Авторство і право володіння. Управління даними. Засоби електронного голосування. Індустрія відеоігор. Організація приватного і державного управління. Інтернет речей. Операції з товарами і сировиною. Благодійність і суспільно корисна діяльність. Нерухомість. Управління ідентифікаційною інформацією. Електронне резидентство. Земельний реєстр. Охорона здоров'я. Енергетика. Боротьба з DDoS-атаками. Освітня сфера. Боротьба з корупцією. Сфери застосування технології розподіленого реєстру в Україні. Земельний реєстр. Електронні торги. Реєстр прав на нерухоме майно. Відкрита платформа електронної демократії. Біотехнології. Фіксація авторських прав.

Назви змістових модулів і тем	Кількість годин						
	Денна форма						
	тижні	усього	у тому числі				
			л	п	лаб.	інд.	с.р.
1	2	3	4	5	6	7	8
Змістовий модуль 1. Складові технології блокчейн							
Тема 1. Введення до технології блокчейн	1-2	22	4		4		14
Тема 2. Як функціонує блокчейн	3-4	24	4		4		16
Тема 3. Токенизація та ICO	5-6	24	4		4		16
Тема 4. Розвиток технології блокчейн	7-8	18	2		2		14
Разом за змістовим модулем 1		88	14		14		60

Змістовий модуль 2. Прикладні аспекти технології блокчейн							
Тема 5. Приватні блокчейни	9-10	22	4		4		14
Тема 6. Децентралізовані додатки (DApps)	11-13	18	2		2		14
Тема 7. Застосування технології блокчейн	14-15	22	4		4		14
Разом за змістовим модулем 2		62	10		10		42
Усього годин		150	24		24		102

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Налаштування оточення для створення локального блокчейну	2
2.	Знайомство із середовищем Remix і альтернативний спосіб запуснути локальний блокчейн Ethereum	2
3.	Створення найпростішого смарт-контракту	2
4.	Створення смарт-контракту «візитка»	2
5.	Наслідування і модифікатори	2
6.	Поняття та основні вимоги токєну ERC20	2
7.	Запуск ICO	4
8.	Знайомство з Hyperledger Fabric	6
9.	Завантаження та запуск смарт контракту в середовищі Hyperledger Fabric	2
	Разом	24

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами.

Перелік питання для визначення рівня засвоєння знань студентами

1. Публічні реєстри відкритого типу.
2. Протоколи консенсусу.
3. Byzantine Fault Tolerance (BFT) протоколи.
4. Реалізація протоколу завдання візантійських генералів.
5. Делегований протокол завдання візантійських генералів.
6. Приклади BFT-протоколів
7. Модифіковані протоколи консенсусу.
8. Публічні реєстри закритого типу.
9. Приватні реєстри з закритим доступом.
10. Громадські організації з делегованим управлінням.
11. Приватні контрольовані блокчейни.

12. Переваги приватних блокчейнів.
13. Платформа Etopum.
14. Дайте коротку характеристику проекту Hyperledger.
15. Сфери використання блокчейну.
16. Блокчейн як послуга (Blockchain-as-a-Service).
17. Сфери застосування технології розподіленого реєстру в Україні.
18. Дайте визначення блокчейну.
19. Що таке хеш-функція.
20. Яку роль відіграє число нонсе?
21. В чому полягає атака 51%.
22. Що таке консенсус.
23. Дайте визначення протоколу.
24. Структура блоку.
25. Що таке майнінг.
26. Комісія за транзакцію.
27. Історія розвитку Ефіріума.
28. Префікне дерево Меркла.
29. Токенізація та ICO.
30. Види токенів.
31. Що таке форк та хардфорк.
32. Чим повна нода відрізняється від полегшеної?
33. Що таке хешрейт?

Приклад екзаменаційного білету

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ			
СВО <i>другий</i> (бакалаврський) <i>рівень</i> <i>051 Економіка «</i>	Кафедра інформаційних систем і технологій	ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1 з дисципліни “ <u>Основи технології блокчейн</u> ”	Затверджую Зав. кафедри Швиденко М.З.
1. Тестові завдання різних типів (максимальна оцінка 10 балів за відповідь на всі тестові завдання)			
2. Задача (максимальна оцінка 10 балів за виконання задачі)			
<ol style="list-style-type: none"> 1) Написати мовою Solidity контракт із заданими згідно варіанту параметрами в середовищі Remix; 2) Перевірити його працездатність; 3) Завантажити файл з кодом в систему для перевірки. 			

8. Методи навчання

Засвоєння матеріалу забезпечується на лекціях, лабораторних заняттях та самостійній роботі у комп'ютерних класах, обладнаних локальними мережами, інтернетом і новітнім програмним забезпеченням. Лекції супроводжуються використанням презентацій, навчальних фільмів та мультимедійного обладнання для полегшення засвоєння матеріалу.

9. Форми контролю

Кожна з форм контролю має особливості й залежить від мети, змісту та характеру навчання. У процесі навчання дисципліни використовуються наступні форми контролю:

- 1. Поточний контроль:** усне опитування (індивідуальне, фронтальне, групове), комп'ютерне тестування, виконання практичних завдань на комп'ютері згідно програми;
- 2. Підсумковий контроль:** тестування та співбесіда за результатами роботи.

10. Розподіл балів, які отримують студенти. Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371)

Поточний контроль		Рейтинг з навчальної роботи $R_{НР}$	Рейтинг з додаткової роботи $R_{ДР}$	Рейтинг штрафний $R_{ШТР}$	Підсумкова атестація (залік)	Загальна кількість балів
Змістовий модуль 1	Змістовий модуль 2					
0-100	0-100	0-70	0-20	0-5	0-30	0-100

Примітки.

Рейтинг з поточної роботи (навчальної, додаткової), штрафний рейтинг та показники підсумкової атестації визначаються відповідно п. 2 та п.4 Положення про екзамени та заліки у Національному університеті біоресурсів і природокористування України, що затверджене Вченою радою НУБіП України « 27 » грудня 2019 р. протокол №5.

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис} = R_{НР} + R_{ат}$.

Загальний рейтинг здобувача вищої освіти із засвоєння дисципліни у балах переводиться у національної оцінки наступним чином:

Шкала оцінювання: національна та ECTS

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	екзаменів	заліків
90-100	відмінно	зараховано
74-89	добре	
60-73	задовільно	
0-59	незадовільно	не зараховано

11. Методичне забезпечення

Електронний навчальний курс, розроблений на базі платформи LMS Moodle, розміщений на навчальному порталі НУБіП України за адресою: <https://elearn.nubip.edu.ua/course/view.php?id=372>

12. Рекомендована література

Основна

1. Дон Тепскотт, Алекс Тепскотт. Блокчейн-революція. Вид-во "Літопис", 2019, 492 с.
2. Юрий Когут. Технології блокчейн та криптовалюта: ризики та кібербезпека. Вид-во "Дакор", 2022, 316 с.

Допоміжна

1. Деніел Роулс. Цифровий брендинг. Вид-во " Фабула", 2020, 256 с.

13. Інформаційні ресурси

1. Blockchain: веб-сайт. URL: <https://www.blockchain.com/> (дата звернення: 27.05.2022)
2. Vitalik Buterin – What is Ethereum and How to Build a Decentralized Future. The Future Thinkers Podcast: веб-сайт. URL: <http://futurethinkers.org/vitalik-buterin-ethereum-decentralized-future/> (дата звернення: 27.05.2022)
3. Алгоритми консенсусу: переваги та недоліки PoS і PoW. CRYPTOTEXTY: веб-сайт. URL: <https://cryptotexty.com/algorithmy-konsensusu-kryptovaljut/> (дата звернення: 27.05.2022)
4. "Попереду планети всієї": які компанії займаються блокчейном в Україні. Економічна правда: веб-сайт. URL: <https://www.epravda.com.ua/projects/fintech/2019/10/9/652378/> (дата звернення: 27.05.2022)
5. Технологія блокчейн уже змінює світ фінансів: як саме. Ліга: Закон: веб-сайт. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ001579 (дата звернення: 27.05.2022)