**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Львівський національний університет імені Івана Франка**

**Факультет економічний**

**Кафедра інформаційних систем у менеджменті**

**Затверджено**

На засіданні кафедри інформаційних систем у менеджменті

економічного факультету

Львівського національного університету імені Івана Франка

(протокол № \_\_\_\_ від \_\_\_\_\_\_\_ 20\_\_ р.)

Завідувач кафедри \_\_\_\_\_\_\_\_\_/В. Приймак/

**Силабус**

**з навчальної дисципліни «Основи block-chain технології»,**

**що викладається в межах другого (магістерського) рівня вищої освіти для здобувачів зі спеціальності 122 «Комп’ютерні науки» освітньо-професійної програми «Консолідована інформація»**

**Львів 2023 р.**

|  |  |
| --- | --- |
| **Назва дисципліни** | Основи block-chain технології |
| **Адреса викладання дисципліни** | м. Львів, проспект Свободи, 18 |
| **Факультет та кафедра, за якою закріплена дисципліна** | Економічний факультет, кафедра інформаційних систем у менеджменті |
| **Галузь знань, шифр та назва спеціальності** | галузі знань 12 «Інформаційні технології»спеціальності 122 «Комп’ютерні науки»освітньо-професійної програми «Консолідована інформація» |
| **Викладачі дисципліни** | Белз Олександра Григорівна, кандидат економічних наук, доцент кафедри інформаційних систем у менеджменті |
| **Контактна інформація викладачів** | oleksandra.belz@lnu.edu.ua, econom.lnu.edu.ua/employee/belz-o-h |
| **Консультації з питань навчання по дисципліні відбуваються** | Консультації в середовищі MS Teams. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача |
| **Сторінка курсу** |  |
| **Інформація про дисципліну** | Курс розроблено таким чином, щоб надати учасникам необхідні знання для вивчення сучасних підходів та принципів роботи блокчейн-систем. У рамках курсу розглядаються ключові аспекти, такі як блоки, алгоритми консенсусу, криптографія та безпека смарт-контрактів. Студенти отримують знання про функціонування інфраструктури блокчейн, процес створення смарт-контрактів на блокчейні Ethereum та важливість безпеки смарт-контрактів. |
| **Коротка анотація дисципліни** | Дисципліна «Основи block-chain технології» є нормативною дисципліною з спеціальності 122 «Комп’ютерні науки» освітньо-професійної програми «Консолідована інформація» для освітньої програми підготовки магістрів, яка викладається в 1 (9) семестрі в обсязі 4 кредити (за Європейською Кредитно-Трансферною Системою ECTS) |
| **Мета та цілі дисципліни** | Метою вивчення дисципліни «Основи block-chain технології» є отримання студентами розуміння технології блокчейн, її потенційних застосувань і вміння використовувати ці знання для розв'язання практичних завдань та проблем. Дисципліна дає розуміння технології блокчейн, її принципів та концепцій, знання про можливості застосування блокчейн-технології в різних сферах, навички розробки додатків на блокчейні та реалізації смарт-контрактів, розуміння проблем безпеки та конфіденційності, пов'язаних з використанням блокчейн |
| **Література для вивчення дисципліни** | 1. Блокчейн і децентралізовані системи: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна – Харків : ПРОМАРТ, 2021. – 458 с.
2. Блокчейн і децентралізовані системи: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. Ч. 2 / П. Кравченко [та ін.]. – Харків : ПРОМАРТ, 2021. – 420 с.
3. Блокчейн і децентралізовані системи: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. Ч. 3 / П. Кравченко [та ін.]. – Харків : ПРОМАРТ, 2021. – 329 с.
4. Ковальчук Л. В. Вступ до технології блокчейн та криптовалют. Частина 1. Теоретичні засади функціонування блокчейн-технологій: навч. посіб [Електронне мережне н авчальне видання] / Л. В. Ковальчук, А. М. Кудін, Н. В. Кучинська. – Київ. КПІ ім. Ігоря Сікорського. – 141 с.
5. Кудин А.М. Блокчейн и криптовалюты на основании «доказательства точности».// Математичне та комп’ютерне моделювання. Серія: технічні науки: збірник наукових праць. Кам’янець-Подільський Національний університет імені Івана Огієнка, вип.15, 2017р., стор. 104-108.
6. Офіційний сайт Bitcoin [Електронний ресурс]. – Режим доступу: https://bitcoin.org/uk/
7. Офіційний сайт Blockchain Academy Mittweida (BCAM) [Електронний ресурс]. – Режим доступу: https://blockchain-academy.hs-mittweida.de
8. Офіційний сайт Ethereum [Електронний ресурс]. – Режим доступу: https://ethereum.org/uk/
9. Офіційний сайт Solidity [Електронний ресурс]. – Режим доступу: https://soliditylang.org/
10. Сервіс моніторингу блоків і транзакцій Bitcoin [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/explorer
11. Сервіс моніторингу блоків і транзакцій Ethereum [Електронний ресурс]. – Режим доступу: https://etherscan.io
 |
| **Обсяг курсу** | **120** годин, з них: 16 години лекцій, 32 годин лабораторних занять та 72 години самостійної роботи |
| **Очікувані результати навчання** | Після завершення цього курсу студент буде: * **Знати**: історію розвитку технології блокчейн, поняття та принцип роботи технології блокчейн, тилему блокчейну, види мереж блокчейн, поняття консенсусу блокчейн, принципи роботи алгоритмів PoW, PoS, DPoS, NPoS, PoSA, PoA, ZKP тощо, структуру блоку, поняття «хешрейт», особливості складність майнінгу в мережі Bitcoin, особливості складність майнінгу в мережі Ethereum (до форку 15 вересня 2022 р.), структуру транзакцій в мережах Bitcoin і Ethereum, суть алгоритму «Дерево Меркла», популярні криптографічні хеш-функції, особливості криптографії в блокчейнах Bitcoin і Ethereum, поняття криптовалюта, стейблкоїн, токен, смарт-контракт, види вразливостей смарт-контрактів, шляхи виправлення вразливостей у смарт-контрактах, поняття та методи аудиту смарт-контрактів
* **Вміти**: працювати з гаманцем MetaMask, розробляти, оптимізовувати та тестувати смарт-контракти, розроблені для блокчейну Ethereum
 |
| **Ключові слова** | Блокчейн, децентралізація, смарт-контракти, криптографія, майнінг, хеш-функції, криптовалюта, стейблкоїн, токен, Bitcoin, Ethereum, алгоритми консенсусу, Дерево Меркла, MetaMask |
| **Формат курсу** | Очний |
| **Теми** | Подано у Схемі курсу |
| **Підсумковий контроль, форма** | Іспит в кінці семестру  |
| **Пререквізити** | Вивчення дисципліни «Основи block-chain технології» забезпечується отриманими знаннями з дисциплін: «Інформаційні і комунікаційні технології», «Комп’ютерні мережі і телекомунікації», «Організація баз даних і знань» |
| **Навчальні методи та техніки, які будуть використовуватися під час викладання курсу** | Лекції з використанням презентацій, демонстрація роботи з програмними системами |
| **Необхідне обладнання** | Вивчення курсу потребує використання такого програмного забезпечення: MetaMask, Remix |
| **Критерії оцінювання (окремо для кожного виду навчальної діяльності)** | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні: 30% семестрової оцінки; максимальна кількість балів 30• контрольні заміри (модулі): 20% семестрової оцінки; максимальна кількість балів 20•іспит: 50% семестрової оцінки; максимальна кількість балів 50Підсумкова максимальна кількість балів – 100 |
| **Питання до заліку чи екзамену.** | 1. Засновнком Bitcoin є
2. Засновнком Ethereum є
3. Перший блок в блокчейні Bitcoin видобуто в
4. Перший блок в блокчейні Ethereum видобуто в
5. Блокчейн 1.0 – це
6. Блокчейн 2.0 – це
7. Блокчейн 3.0 – це
8. Нода – це
9. Трилема блокчейну – це ідея про те, що блокчейнам важко досягти оптимальних рівнів усіх трьох властивостей одночасно, а саме
10. Шардінг – це
11. До рішень рівня 1, які вирішують трилему блокчейну, належать
12. До рішень рівня 1, які вирішують трилему блокчейну, належать
13. До рішень рівня 2, які вирішують трилему блокчейну, належать
14. Види мереж блокчейн
15. Транзакційна прозорість в мережі блокчейн передбачає, що всі транзакції, здійснені на блокчейні, є публічними та доступними для перегляду
16. Сайдчейн - це технологія, яка передбачає, що
17. Канал стану - це технологія, яка передбачає, що
18. Вкладені блокчейни - це технологія, яка передбачає, що
19. Алгоритми консенсусу блокчейну стосуються
20. Алгоритми консенсусу блокчейну стосуються
21. Нонс (nonce) - це
22. У мережах з консенсусом Proof of Work (PoW) винагороду за виконану роботу отримує
23. У мережах з консенсусом Proof of Stake (PoS) більший шанс стати валідатором має
24. У мережах з консенсусом Delegated Proof of Stake (DPoS) більший шанс стати валідатором має
25. У мережах з консенсусом Nominated Proof of Stake (NPoS) більший шанс стати валідатором має
26. У мережах з консенсусом Proof of Authority (PoA) більший шанс стати валідатором має
27. Переваги алгоритму консенсусу Proof of Work (PoW)
28. Недоліки алгоритму консенсусу Proof of Work (PoW)
29. Переваги алгоритму консенсусу Proof of Stake (PoS)
30. Недоліки алгоритму консенсусу Proof of Stake (PoS)
31. Переваги алгоритму консенсусу Proof of Authority (PoA)
32. Недоліки алгоритму консенсусу Proof of Authority (PoA)
33. Структура даних, що зберігаються всередині блоку, залежить від
34. Хешрейт вимірюється в
35. У мережах з консенсусом Proof of Work (PoW) для управління часом знаходження блоків в мережі використовується
36. В мережі Bitcoin після формування кожних 210 000 блоків запрограмовано
37. В мережі Bitcoin складність коригується кожні
38. Дерево Меркла (хеш-дерево) - це
39. Корінь Меркла (кореневий хеш дерева Меркла)- це обов'язковий елемент
40. Термін «хешрейт» має таке значення
41. Типи транзакцій в блокчейні Ethereum
42. Дерева Меркла дають змогу
43. В блокчейні Ethereum використовуються такі хеш-дерева
44. Хешування - це
45. Стійкість до колізії означає
46. Стійкість до знаходження першого першовзору означає
47. Стійкість до знаходження другого першовзору означає
48. External owned accounts (EOA) в блокчейні Ethereum - це
49. Contract accounts (CA) в блокчейні Ethereum - це
50. External owned accounts (EOA) в блокчейні Ethereum має такі ключі
51. Contract accounts (CA) в блокчейні Ethereum має такі ключі
52. Довжина приватного ключа в блокчейні Ethereum
53. Довжина відкритого ключа в блокчейні Ethereum
54. Довжина адреси в блокчейні Ethereum (з префіксом)
55. Криптографічна хеш-функція повинна відповідати таким властивостям
56. Типи акаунтів в блокчейні Ethereum
57. У процесі створення адреси в блокчейні Bitcoin використовуються такі хеш-функції
58. Криптовалюта (Cryptocurrency) - це
59. Токен (криптовалютний) - це
60. Токен автентифікації - це
61. Стейблкойн, або стейблкоїн (stablecoin ) - це
62. Фіатні стейблкоїни - це такі, що
63. Товарні стейблкоїни - це такі, що
64. Криптовалютні стейблкоїни - це такі, що
65. Алгоритмічні стейблкоїни - це такі, що
66. Сеньйоражні стейблкоїни - це такі, що
67. Токени додатків - це такі, що
68. Токени-жетони - це такі, що
69. Утилітарні токени - це такі, що
70. Токени користувача - це такі, що
71. Токени апкойни (Appcoins) - це такі, що
72. Токени-акції - це такі, що
73. Кредитні токени - це такі, що
74. Унікальні токени (Non-fungible token, NFT) - це такі, що
75. Динамічні токени (dNFT) - це такі, що
76. Смарт-контракт - це
77. Типи стейблкоїнів за способами їхнього забезпечення
78. Типи централізованих стейблкоїнів
79. Типи децентралізованих стейблкоїнів
80. Види токенів
81. Об'єкти смарт-контракту
82. Види вразливостей смарт-контрактів
83. Методи аудиту смарт-контрактів
84. Методи функціонального тестування смарт-контрактів
85. В Solidity для змінної "uint public myUint" вираз "myUint == 1" означає
86. В Solidity для змінної "uint public myUint" вираз "myUint -- 1" означає
87. В Solidity для змінної "uint public myUint" вираз "myUint --" означає
88. В Solidity для змінної "uint public myUint" вираз "myUint =- 1" означає
89. В Solidity для змінної "uint public myUint" вираз "myUint != 1" означає
90. В Solidity для змінної "uint public myUint" вираз "myUint -= 1" означає
91. В Solidity для змінної "uint public myUint" вираз "myUint = myUint - 1" означає
92. В Solidity для змінної "int public myInt" вираз "myInt =- 1" означає
93. В Solidity метод ".push" означає
94. В Solidity видимість функції "external" означає, що
95. В Solidity видимість функції "internal" означає, що
96. В Solidity видимість функції "private" означає, що
97. В Solidity видимість функції "public" означає, що
98. В Solidity вбудований модифікатор функцій "view" означає, що
99. В Solidity вбудований модифікатор функцій "pure" означає, що
100. В Solidity вбудований модифікатор функцій "payable" означає, що
101. В Solidity вбудована функція "require" - це
102. В Solidity вбудована функція "receive" - це
103. В Solidity вбудована функція "fallback" - це
104. В Solidity метод ".transfer" виконує таку дію
105. В Solidity метод ".balance" виконує таку дію
106. В Solidity метод "msg.sender" виконує таку дію
107. В Solidity чим відрізняється змінна, визначена як "address", від змінної, визначеної як "address payable"
108. В Solidity метод "msg.value" виконує таку дію
109. В Solidity вбудований модифікатор функцій "virtual" означає, що
110. В Solidity вбудований модифікатор функцій "override" означає, що
111. Які типи даних в Solidity існують
 |
| **Опитування** | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу |