Силабус курсу
БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУВАННЯ

Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Наталія Яцків
Контактна інформація	jng@wunu.edu.ua

Опис дисципліни

Анотація до курсу. Курс "Блокчейн: математичні проблеми та застосування" спрямований на вивчення теоретичних аспектів та математичних основ технології блокчейн, а також розгляд її реальних застосувань. Головні аспекти курсу включають наступне:

1. Теорія блокчейну. Учасники отримають глибше розуміння технології блокчейн, включаючи поняття децентралізації, розподіленого реєстру, геш-функцій, криптографії та інших математичних основ.
2. Консенсус-алгоритми.Курс докладно розглядає різні методи досягнення консенсусу в мережі блокчейн, такі як Proof of Work (PoW) та Proof of Stake (PoS), та їхню математичну базу.
3. Математичні проблеми в блокчейні. Курс досліджує математичні виклики та проблеми, пов'язані з безпекою та ефективністю мереж блокчейн, включаючи проблему подвійного витрати (double-spending), атаки 51%, анонімність та інші.
4. Застосування в практиці. Учасники дізнаються, як застосовувати свої математичні знання в реальних проектах та розвивати рішення на базі технології блокчейн.
5. Перспективи блокчейн. Курс вивчає тренди та майбутні перспективи розвитку технології блокчейн та її вплив на світову економіку та суспільство.

Цей курс розроблений для тих, хто має інтерес до глибокого розуміння математичних аспектів блокчейну та хоче долучитися до розробки та впровадження рішень на базі цієї технології. Він підходить для студентів, фахівців з інформатики, математики та інших відповідних галузей, які бажають поглибити свої знання у цій захоплюючій області.

Метою курсу «Блокчейн: математичні проблеми та застосування» є формування у студентів цілісного уявлення про суть технології блокчейн та переваги її використання в різних сферах діяльності.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Технологія блокчейн	Аналізувати стан розвитку технології блокчейн та її застосування	Поточне опитування
2/0	Архітектура блокчейн	описувати переваги та обмеження технології блокчейн	Поточне опитування
2/2	Типи блокчейна	пояснювати різницю між типами блокчейну	Поточне опитування
2/2	Децентралізація	пояснювати переваги децентралізації	Поточне опитування

2/2	Симетрична криптографія в блокчейн	розуміти та застосовувати симетричні криптографічні алгоритми	Поточне опитування
2/2	Асиметрична криптографія в блокчейн	розуміти та застосовувати асиметричні криптографічні алгоритми	Поточне опитування
2/2	Цифрові підписи в блокчейн	зрозуміти та астосовувати цифрові підписи	Поточне опитування
2/0	Математика еліптичних кривих.	розробляти алгоритми шифрування на основі еліптичних кривих	Поточне опитування, тестування
2/0	Криптографічні конструкції та технологія блокчейн	демонструвати розуміння доказів з нульовим знанням	Поточне опитування
2/2	Алгоритми консенсусу	демонструвати знання алгоритмів консенсусу	Поточне опитування
2/0	Архітектура біткоіна	аналізувати дані транзакцій в мережі біткоін	Поточне опитування
2/2	Структура блокчейн	розуміти структуру блокчейн	Поточне опитування
2/1	Конфіденційність блокчейну	знати методи досягнення конфіденційності в блокчейні	Поточне опитування
2/0	Безпека блокчейну	використовувати інструменти та механізм аналізу безпеки	Поточне опитування
2/0	Застосування блокчейну та перспективи	застосовувати блокчейн для підвищення безпеки IoT	Поточне опитування, тестування

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. 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.
4. 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.
5. Song, J. *Programming bitcoin: Learn how to program bitcoin from scratch*. O'Reilly Media, 2019, 321 p.
6. V.Yatskiv, N.Yatskiv, O. Bandrivskyi. "Proof of Video Integrity Based on Blockchain", in *Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on*, 2019, pp. 431-434.
7. A. Panarello, N.Tapas, G.Merlino, F.Longo, A.Puliafito "Blockchain and IoT integration: A systematic survey". *Sensors, vol.*18(8)**,** *2575,* pp.1-37, 2018.
8. M. Salimitari, M. Chatterjee. "An Overview of Blockchain and Consensus Protocols for IoT Networks". arXiv preprint arXiv:1809.05613, 2018.
9. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, R.Ranjan. "IoT Chain: Establishing trust in the internet of things ecosystem using blockchain". *IEEE Cloud Computing*, vol.5(4), pp.12-23, 2018.
10. Liu, X., Yang, H., Li, G., Dong, H., & Wang, Z. (2021). A blockchain-based auto insurance data sharing scheme. *Wireless Communications and Mobile Computing*, Volume 2021, Article ID 3707906 https://doi.org/10.1155/2021/3707906

11. 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

12. S.Son,J.Lee,M.Kim,S.Yu,A.K.Das,andY.Park,"Designof secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, 2020. – pp. 192177–192191.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
30 %	40 %	30 %
1. Усне опитування на заняттях – max 8*3=24 балів. 2. Письмова робота – max 52 балів. 3. Практичне завдання – max 4*6=24 балів	1. Усне опитування на заняттях – max 7*3=21 балів. 2. Письмова робота – max 55 балів. 3. Практичне завдання – max3*8=24 балів	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 балів

Шкала оцінювання:

ECTS	**Бали**	**Зміст**
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом