МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра обчислювальної математики

Затверджено
на засіданні
кафедри обчислювальної математики
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № _1_ від _29 серпня_ 2023 р.)

Завідувач кафедри

Роман ХАПКО

Силабус з навчальної дисципліни «Вступ до блокчейн-технологій», що викладається в межах ОПП Прикладна математика першого (бакалаврського) рівня вищої освіти для здобувачів зі спеціальності 113 – Прикладна математика

Львів 2023 р.

Назва дисципліни	Вступ до блокчейн-технологій
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра обчислювальної математики
Галузь знань, шифр та назва спеціальності	113 Прикладна математика
Викладачі дисципліни	Лаврик Святослав Володимирович, асистент кафедри обчислювальної математики
Контактна інформація викладачів	sviatoslav.lavryk@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка, каб. 262. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
Сторінка курсу	
Інформація про дисципліну	Дисципліна «Вступ до блокчейн-технологій» є вибірковою дисципліною з спеціальності 113 – прикладна математика для освітньої програми «Прикладна математика», яка викладається в 8-му семестрі (4 кредити ECTS).
Коротка анотація дисципліни	Курс розроблено таким чином, щоб ознайомити студентів з принципами побудови розподілених та децентралізованих систем, алгоритмічними основами блокчейн систем, методами та інструментами розробки смарт-контрактів Ethereum та Web 3 аплікацій.
Мета та цілі дисципліни	Метою вивчення вибіркової дисципліни «Вступ до блокчейн-технологій» є освоєння студентами принципів побудови розподілених та децентралізованих систем, алгоритмічних основ блокчейн систем, методів та інструментів розробки смарт-контрактів Ethereum та Web 3 аплікацій.
Література для вивчення дисципліни	**Основна література** 1. Imran Bashir. Mastering Blockchain, 4th edition /Imran Bashir// Packt – 2023 2. Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography / Darrel Hankerson, Alfred Menezes, Scott Vanstone // Springer-Verlag –2004 3. https://bitcoin.org/en/bitcoin-paper 4. https://ethereum.github.io/yellowpaper/paper.pdf **Допоміжна література:** 1. https://ethereum.org/en/developers/docs 2. https://www.openssl.org/docs/

	3. https://remix-ide.readthedocs.io/en/latest/ 4. https://docs.soliditylang.org/en/v0.8.24/ 5. https://archive.trufflesuite.com/docs/ 6. https://docs.ethers.org/v5/ 7. https://docs.openzeppelin.com/
Обсяг курсу	Загальний обсяг: 120 годин (аудиторних занять: 56 год., з них 28 год. лекцій та 28 год. лабораторних робіт; самостійної роботи: 64 год).
Очікувані результати навчання	Після завершення цього курсу студент буде : Знати: – принципи побудови розподілених та децентралізованих систем; – основи криптографічних алгоритмів, що використовують в блокчейн-технологіях; – основи алгоритмів децентралізованого консенсусу, що використовують в блокчейн-технологіях; – архітектуру блокчейн-системи Ethereum, основні поняття та засоби мови програмування Solidity; – принципи та інструменти побудови смарт-контрактів, токенів в Ethereum; – основи побудови Web 3 аплікацій з використанням бібліотеки ethers.js та інших; Вміти: – аналізувати і розуміти особливості архітектури різних блокчейн-систем; – розробляти смарт-контракти, токени та інші типи децентралізованих аплікацій в системі Ethereum; – розробляти Web 3 аплікації з використанням бібліотеки ethers.js та інших;
Ключові слова	Розподілені системи, децентралізовані системи, криптографія, алгоритми консенсусу, блокчейн, Ethereum, Web 3, Solidity.
Формат курсу	Очний Проведення лекцій, лабораторних занять і консультацій.
Теми	Подано нижче у таблиці Схема курсу «Вступ до блокчейн-технологій».
Підсумковий контроль, форма	Залік.
Пререквізити	Для вивчення курсу студенти потребують базових знань з: - теорії алгоритмів та структур даних; - програмування;
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції (лекції-бесіди, лекції-розповіді). Індивідуальні завдання.

<table>
<tr><td>Необхідне обладнання</td><td>Комп’ютер із програмним забезпеченням Visual Studio, Visual Studio Code, openssl, Node.js, доступ до Internet мережі.</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>Оцінювання проводиться за 100-бальною шкалою.
<table>
<tr><th colspan="2" rowspan="2">Оцінка за шкалою ECTS</th><th rowspan="2">Оцінка в балах</th><th colspan="3">Оцінка за національною шкалою</th></tr>
<tr><th colspan="2">Екзамен, диференційований залік</th><th>залік</th></tr>
<tr><td>A</td><td>Відмінно</td><td>100 - 90</td><td>Відмінно</td><td>5</td><td rowspan="5">зараховано</td></tr>
<tr><td>B</td><td>Дуже добре</td><td>81- 89</td><td rowspan="2">Добре</td><td rowspan="2">4</td></tr>
<tr><td>C</td><td>Добре</td><td>71 -80</td></tr>
<tr><td>D</td><td>Задовільно</td><td>61 - 70</td><td rowspan="2">Задовільно</td><td rowspan="2">3</td></tr>
<tr><td>E</td><td>Достатньо</td><td>51- 60</td></tr>
<tr><td>FX (F)</td><td>Незадовільно</td><td>0 - 50</td><td>Незадовільно</td><td>2</td><td>не зараховано</td></tr>
</table>
Впродовж семестру студент може отримати 100 балів. З них:
- за роботу на лабораторних заняттях: максимальна кількість – 100 балів (4 програми (індивідуальні завдання) по 25 балів); для кожного завдання встановлено терміни здачі. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (кожен блок тем на 5 балів менше).
Підсумкова максимальна кількість балів 100.

Критерії оцінювання індивідуальних завдань:
25 балів – студент повністю виконав умови завдання, алгоритм реалізовано правильно, відповідає на всі запитання, пов'язані з тематикою завдання, проводить чіткий аналіз та порівняння отриманих результатів, пропонує інші підходи до вирішення поставленого завдання;
20-24 бали – студент повністю виконав умови завдання, на деякі запитання, алгоритм реалізовано правильно, пов'язані з тематикою завдання, відповідає з незначними неточностями, проводить аналіз отриманих результатів з незначними неточностями;
15-19 балів – студент виконав завдання з незначними помилками, але самостійно їх виправляє, якщо на них вкаже викладач, на деякі запитання, пов'язані з тематикою завдання, відповідає з неточностями, проводить аналіз отриманих результатів з неточностями;
5-14 балів – студент виконав завдання частково, алгоритм реалізовано з помилками, які частково може виправити, якщо на них вкаже викладач, на запитання відповідає з помилками, проводить аналіз отриманих результатів з помилками;
2-5 балів – студент виконав завдання частково, алгоритм реалізовано з помилками, які самостійно не може виправити, переважно не</td></tr>
</table>

	відповідає на запитання; **1 бал** – студент виконав завдання частково з грубими помилками, які самостійно не може виправити, демонструє незнання матеріалу; **0 балів** – студент не виконав завдання. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані за індивідуальні завдання. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу «Вступ до блокчейн-технологій»

Тиждень	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в інтернеті	Завдання, год.	Термін виконання
1	**Тема 1.** Поняття про розподілені та децентралізовані системи, децентралізований консенсус, основні проблеми побудови децентралізованих систем	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 2. Властивості розподілених систем – consistency, availability, partition	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу	1 тиждень

	tolerance. CAP теорема.			(2 год.)	
2	**Тема 3.** Вступ до криптографії. Основні криптографічні задачі. Поняття криптографічних примітивів. Криптографічні хеш-функції.	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 3. Базові команди openssl. Приклади використання хеш-функції SHA256 в openssl.	лабораторне (2 год.)	[1], допоміжна [2]	Виконання практичних прикладів (2 год.)	під час заняття
3	**Тема 4.** Основи симетричної криптографії. Потокові та блочні шифри. Алгоритми DES, AES, їх особливості.	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 4. Приклади використання алгоритму AES в openssl. Поняття транспортного кодування (Base64).	лабораторне (2 год.)	[1], допоміжна [2]	Виконання практичних прикладів (2 год.)	під час заняття
4	**Тема 5.** Основи асиметричної криптографії. Алгоритми RSA, ECC. Алгоритми обміну ключами (Diffie-Hellman)	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 5. Приклади використання алгоритів RSA, ECC та Diffie-Hellman key exchange в openssl. *(Індивідуальне завдання №1. Обмін захищеними повідомленнями з використанням openssl та RSA)*	лабораторне (2 год.)	[1], допоміжна [2]	Виконання індивідуального завдання №1 (4 год.)	під час заняття 2 тижні
5	**Тема 6.** Алгоритми децентралізованого консенсусу. Типи стійкості алгоритмів – CFT, BFT. Практичні обмеження стійкості алгоритмів.	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 7. Алгоритми консенсусу на основі Proof-of-Work, Proof-of-Stake. Поняття транзакції та децентралізованого леджеру.	лекція (2 год.)	[3]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
6	**Тема 7.** Приклад обчислювальної складності Proof-of-Work на основі хеш-функції SHA256. *(Індивідуальне завдання №2. Proof-of-Work з використанням SHA256)* *Здача індивідуального завдання*	лабораторне (2 год.)	[3]	Виконання індивідуального завдання №2 (4 год.)	під час заняття 2 тижні під час

	№1				заняття
	Тема 8. Основи побудови блокчейн системи Ethereum, основні інструменти (адреси, гаманці, seed phrases), поняття про смарт-контракти.	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
7	**Тема 8.** Приклади розробки простих смарт-контрактів з використанням Remix.	лабораторне (2 год.)	[1], допоміжна [3]	Виконання практичних прикладів (2 год.)	під час заняття
	Тема 9. Ознайомлення з мовою програмування Solidity.	лекція (2 год.)	допоміжна [4]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
8	**Тема 9.** Приклади розробки складніших смарт-контрактів з використанням Remix, приклади тестових мереж Ethereum	лабораторне (2 год.)	допоміжна [3]	Виконання практичних прикладів (2 год.)	під час заняття
	Тема 9. Приклади розробки складніших смарт-контрактів з використанням Truffle і Ganache, приклади blockchain explorers.	лабораторне (2 год.)	допоміжна [5]	Виконання практичних прикладів (2 год.)	під час заняття
9	*Здача індивідуального завдання №2*	лабораторне (2 год.)	[3]	Виконання індивідуального завдання (2 год.)	під час заняття
	Тема 10. Ознайомлення з бібліотеками ethers.js та платформою Truffle.	лекція (2 год.)	допоміжна [5], [6]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
10	**Тема 10.** Приклади взаємодії з Ethereum засобами ethers.js – створення та підпис транзакцій, моніторинг транзакцій.	лабораторне (2 год.)	допоміжна [6]	Виконання практичних прикладів (2 год.)	під час заняття
	Тема 10. Приклади взаємодії з Ethereum засобами Truffle – створення, тестування та деплоймент смарт-контрактів. *(Індивідуальне завдання №3. Створення смарт-контракту в Ethereum для обміну повідомленнями)*	лабораторне (2 год.)	допоміжна [5], [6]	Виконання індивідуального завдання №3 (4 год.)	під час заняття 2 тижні

11	**Тема 11.** Поняття про токени, взаємозамінність (fungibility) токенів	лекція (2 год.)	допоміжна [1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 11. Приклади створення токенів в Ethereum засобами Truffle	лабораторне (2 год.)	допоміжна [5]	Виконання практичних прикладів (2 год.)	під час заняття
12	**Тема 12.** Поняття про NFT (non-fungible tokens), стандарти токенів ERC-20, ERC-721, ERC-1155	лекція (2 год.)	допоміжна [1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Тема 12. Приклади створення NFT токенів в Ethereum засобами Truffle. Бібліотека OpenZeppelin. *(Індивідуальне завдання №4. Створення токену в Ethereum)* *Здача індивідуального завдання №3*	лабораторне (2 год.)	допоміжна [5], [7]	Виконання індивідуального завдання №4 (4 год.)	під час заняття 2 тижні під час заняття
13	**Тема 13.** Поняття про Web 3 аплікації, використання бібліотеки ethers.js у Web-аплікаціях.	лекція (2 год.)	допоміжна [6]	Виконання практичних прикладів (2 год.)	під час заняття
	Тема 13. Приклади використання бібліотеки ethers.js у Web-аплікаціях	лабораторне (2 год.)	допоміжна [6]	Виконання практичних прикладів (2 год.)	під час заняття
14	**Тема 14.** Аспекти побудови систем з використанням блокчейну, поняття про on-chain та ofi-chain. Підсумки курсу.	лекція (2 год.)	[1]	Опрацювання лекційного матеріалу (2 год.)	1 тиждень
	Здача індивідуального завдання №4	лабораторне (2 год.)	допоміжна [5], [7]	Виконання індивідуального завдання (2 год.)	під час заняття