Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Технології Блокчейн

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	*Другий (магістерський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 Комп'ютерна Інженерія*
Освітня програма	*ОНП Системне програмування та спеціалізовані комп'ютерні системи*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1-й курс магістратури, весняний семестр*
Обсяг дисципліни	*5 кредитів ECTS*
Семестровий контроль/ контрольні заходи	*2-й семестр: екзамен*
Розклад занять	*http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції і лабораторні роботи: к.т.н., доцент кафедри СПіСКС Щербина Олександр Андрійович, moodlemoot@i.ua, тел. +38(044)204-99-33, асистент кафедри СПіСКС Щербина Богдан Олександрович, bogdan.shcherbina11@gmail.com, тел. +38(044)204-99-33*
Розміщення курсу	*https://scs-kpi.pp.ua/course/view.php?id=323* , https://campus.kpi.ua ,

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Навчальна дисципліна «Технології Блокчейн» має сформувати у студентів компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з роботою з блокчейн-системами та систем розподіленого консенсусу.

Метою навчальної дисципліни є ознайомлення студентів з сучасними технологіями і засобами розробки криптовалютних систем; набуття ними практичних навичок роботи з технологіями та принципами, що лежать в їх основі, таких як криптографія, комп'ютерні мережі, теорія інформації та економіка.

Предмет дисципліни – теоретичні та практичні основи створення та вивчення існуючого програмного коду для роботи з криптовалютними протоколами.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за освітньою програмою)

***Пререквізити**. Дисципліні «Технології Блокчейн» передують дисципліни , «Теорія інформації та кодування», «Економіка», та «Комп'ютерні мережі» навчального плану ОКР «Бакалавр» та дисципліна «Криптографія» освітньо-наукової підготовки магістрів навчального плану другого магістерського рівня вищої освіти за спеціалізацією «Спеціалізовані комп'ютерні системи».*

***Постреквізити.** Результати вивчення дисципліни не будуть використовуватися при вивченні наступних дисциплін в останньому семестрі підготовки магістрів.*

3. Зміст навчальної дисципліни

Тема 1. Вступ. Економічні та ідеологічні причини виникнення Біткойну. Гроші. Примітивні гроші. Гроші як метал. Гроші як гарантія від держави. Стабільна валюта.

Тема 2. Що таке Біткойн. Історія Біткойну. Користувачі Біткойну.

Тема 3. Як працює Біткойн. Транзакції. Блоки. Майнінг. Блокчейн.

Тема 4. Біткойн клієнт. Референтна імплементація. Робота з клієнтом мережі. Альтернативні клієнти.

Тема 5. Ключі, адреси, гаманці. Публічні та приватні ключі та криптографія. Криптографія еліптичних кривих. Біткойн адреси.

Тема 6. Транзакції. Життєвий цикл транзакцій. Структура, входи та виходи транзакцій. Скрипти та скриптова мова програмування.

Тема 7. Скрипти та скриптова мова програмування транзакцій.

Тема 8. Біткойн мережа. Архітектура мережі. Типи та ролі вершин мережі. Пули транзакцій.

Тема 9. Блокчейн. Структура блоку. Заголовок блоку. Ідентифікатори блоку: хеш заголовку блоку та висота блоку.

Тема 10. Зв'язок блоків в блокчейн. Дерева Меркла.

Тема 11. Майнінг і консенсус. Децентралізований консенсус. Незалежна верифікація транзакцій. Агрегація транзакцій в блоки.

Тема 12. Нагороди за блоки, комісії. Алгоритм "Proof-Of-Work". Складність та її коригування. Валідація блоку.

Тема 13. Майнінг та гонки хеш-потужностей. Атаки на консенсус.

Тема 14. Альтернативні блокчейни та їх застосування.

Тема 15. Безпека біткойну. Принципи безпеки. Рекомендації до безпеки.

Тема 16. Для чого потрібен біткойн. Збереження купівельної спроможності. Індивідуальна автономія.

Тема 17. Потенціальні покращення та нові розробки.

Тема 18. Потенціальні проблеми та вектори атак.

4. **Навчальні матеріали та ресурси**

Базова література

1. *Saifedean Ammous. Bitcoin Standard. The Decentralized Alternative to Central Banking Wiley; 1st edition, 2018, 304 p.*

2. *Mastering Bitcoin / Andreas Antonopoulos. [Електронний ресурс]. Режим доступу: https://github.com/bitcoinbook/bitcoinbook.*

Допоміжна література

3. *Референтна імплементація. [Електронний ресурс]. Режим доступу: https://github.com/bitcoin/bitcoin*

4. *Дон Тапскотт, Алекс Тапскотт. Блокчейн-революція. Видавництво Літопис, 2019, 492 с.*

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1 Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	***Вступ.*** *Економічні та ідеологічні причини виникнення Біткойну. Гроші. Примітивні гроші. Гроші як метал. Гроші як гарантія від держави. Стабільна валюта.*
2	***Що таке Біткойн.*** *Історія Біткойну. Користувачі Біткойну.*
3	***Як працює Біткойн.*** *Транзакції. Блоки. Майнінг. Блокчейн.*
4	***Біткойн клієнт.*** *Референтна імплементація. Робота зі клієнтом мережі. Альтернативні клієнти.*
5	***Ключі, адреси, гаманці.*** *Публічні та приватні ключі та криптографія. Криптографія еліптичних кривих. Біткойн адреси.*
6	***Транзакції.*** *Життєвий цикл транзакцій. Структура, входи та виходи транзакцій. Скрипти та скриптова мова програмування.*
7	***Скрипти та скриптова мова програмування транзакцій****. Основні види скриптів. Конструювання скриптів (замикання та розмикання). Неповнота за Т'юрінгом.*
8	***Біткойн мережа.*** *Архітектура мережі. Типи та ролі вершин мережі. Пули транзакцій.*
9	***Блокчейн.*** *Структура блоку. Заголовок блоку. Ідентифікатори блоку: хеш заголовку блоку та висота блоку.*
10	***Зв'язок блоків в блокчейн.*** *Дерева Меркла.*
11	***Майнінг і консенсус.*** *Децентралізований консенсус. Незалежна верифікація транзакцій. Агрегація транзакцій в блоки.*
12	***Нагороди за блоки, комісії.*** *Алгоритм "Proof-Of-Work". Складність та її коригування. Валідація блоку.*
13	***Майнінг та гонки хеш-потужностей.*** *Атаки на консенсус.*
14	***Альтернативні блокчейни.*** *Альтернативні, валюти та застосування. Альтернативні алгоритми консенсусу.*
15	***Безпека біткойну.*** *Принципи безпеки. Рекомендації до безпеки.*
16	***Для чого потрібен біткойн.*** *Збереження купівельної спроможності. Індивідуальна автономія.*

17	***Потенціальні покращення та нові розробки.*** *Багатоцільовий майнінг. Приватність транзакцій.*
18	***Потенціальні проблеми та вектори атак.*** *Атаки на системи розподіленого консенсусу.*

5.2 ***Лабораторні роботи***

№ з/п	*Назва теми заняття та перелік основних питань*
1	*Вступ та окреслення цілей курсу. Знайомство та встановлення існуючої реалізації біткойн-протоколу.*
2	*Створення програми для зберігання та синхронізації блоків.*
3	*Створення програми для валідації блоків.*
4	*Створення програми для майнінгу.*
5	*Створення програми для виконання алгоритму Proof-Of-Work.*
6	*Створення простого механізму транзакцій.*
7	*Створення скриптової мови та простих скриптів для транзакцій.*
8	*Поєднання елементів створених програм для створення власної системи розподіленого консенсусу.*
9	*Введення додаткових ускладнень до алгоритму консенсусу для створеної програми.*

6. Самостійна робота студента

Самостійна робота студентів при вивченні даної дисципліни має дві складові: теоретичну і практичну. Теоретична складова полягає у закріпленні матеріалу, що викладається під час лекційного курсу, а також самостійного вивчення рекомендованої літератури.

Практична складова полягає у створенні студентом клієнта власної системи розподіленого консенсусу та його синхронізація з клієнтами своїх одногрупників.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Система вимог, які ставляться перед здобувачем освіти:

- *відвідування лекційних та лабораторних занять є обов'язковою складовою вивчення матеріалу;*
- *на лекції викладач користується власним презентаційним матеріалом;*
- *на лекції заборонено відволікати викладача від викладання матеріалу, усі питання, уточнення тощо студенти задають в кінці лекції у відведений для цього час;*
- *на лекціях забороняється використовувати ноутбуки та смартфони з метою, яка не стосується занять;*

- *лабораторні роботи проходять у формі комп'ютерного практикуму. Основним завданням циклу лабораторних занять є робота зі створення і використання власної системи розподіленого консенсусу. При цьому студенти мають не тільки створити власний клієнт, а й синхронізувати його у мережу з розробками своїх одногрупників.*

заохочувальні бали виставляються за:

- *активність на лекціях;*
- *участь у факультетських та інститутських олімпіадах з навчальних дисциплін;*
- *участь у конкурсах робіт; підготовку оглядів наукових праць, презентацій по одній із тем дисципліни тощо;*
- *кількість заохочуваних балів не більше 10;*

штрафні бали виставляються за: невчасну здачу лабораторних робіт.

Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Рейтинг студента з дисципліни складається із балів стартового рейтингу (протягом семестру) та балів за екзамен. Бали стартового рейтингу протягом семестру студент отримує за:

- *виконання і захист лабораторних робіт;*

Критерії нарахування балів:

Бали нараховуються за виконання та захист лабораторних робіт. Протягом семестру студенти виконують 9 лабораторних робіт. Виконання робіт оцінюється наступним чином:

Таблиця 1. Максимальна можлива кількість балів за кожну роботу

Номер роботи	*Максимальна кількість балів*
1	*5*
2	*10*
3	*10*
4	*10*
5	*10*
6	*15*
7	*15*
8	*20*
9	*5*

Таким чином, студент за семестр може набрати 100 балів, з яких і складається його підсумкова оцінка, якщо вона виставляється за поточною успішністю. Якщо екзамен проводиться за звичайною процедурою, то підсумкова оцінка обчислюється як середнє арифметичне зазначеного вище балу та 100-бальної оцінки на екзамені.

Таблиця 2. Переведення рейтингових балів до оцінок за університетською шкалою

Бали	***Оцінка***
95-100	*відмінно*
85-94	*дуже добре*
75-84	*добре*
65-74	*задовільно*
60-64	*достатньо*
Менше 60	*незадовільно*
Є незараховані лабораторні роботи та/або створення власного курсу на оцінку «незадовільно»	*не допущено*

Робочу програму навчальної дисципліни (силабус):

Складено доцентом кафедри СПіСКС, к.т.н., доцентом Щербиною Олександром Андрійовичем і асистентом кафедри СПіСКС, Щербиною Богданом Олександровичем,

Ухвалено кафедрою СПіСКС (протокол №6 від 03.01.2024),

Погоджено методичною комісією факультету ПМ (протокол № 6 від 26.01.2024).