Силабус освітнього компонента
Програма навчальної дисципліни

Технології блокчейн

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Комп'ютерна математика і аналіз даних

Рівень освіти
Магістр

Тип дисципліни
Профільна, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

Дубініна Оксана Миколаївна

Oksana.Dubinina@khpi.edu.ua
Доктор педагогічних наук, кандидат технічних наук, професор, професор кафедри комп'ютерної математики і аналізу даних НТУ «ХПІ».

Досвід роботи – понад 30 років. Автор і співавтор понад 100 наукових та навчально-методичних публікацій. Лектор з дисциплін: «Вища математика», «Технологія блокчейн».
h-index = 2 in Scopus –
https://www.scopus.com/authid/detail.uri?authorId=57194556274
h-index = 6, i10-index = 2 in Google Scholar –
https://scholar.google.com.ua/citations?user=-Qz9nSsAAAAJ&hl=ru
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна охоплює основні технічні та фундаментальні аспекти технології блокчейн і рівні застосунків, надаючи здобувачам магістерського рівня підготовки можливість глибоко розібратися в основах. Особливість курсу полягає в тому, що матеріал викладається на стику принципів роботи, переваг і ризиків інноваційних інформаційних технологій. У курсі передбачено два змістових модулі. Опанування дисципліни передбачає формування сучасного інженерного мислення, навчання основним технологічним засобам, необхідним для дослідження, аналізу та моделювання процесів при пошуку оптимальних рішень та виборі найкращих засобів реалізації цих рішень, прийомам дослідження та розв'язку математично формалізованих задач, вміння провести аналіз і синтез отриманих результатів та вхідних даних.

Мета та цілі дисципліни

Набуття студентами компетентностей, необхідних для подальшої роботи шляхом опанування технічних деталей функціонування механізмів блокчейну, ознайомлення з новими концепціями, які стосуються стеку децентралізованих технологій, розвиток логічного і алгоритмічного

мислення студентів; опанування студентами методів дослідження і аналізу прикладних та інженерних завдань. У результаті засвоєння дисципліни зокрема формуються: здатність розуміти послуги безпеки та способи їх надання; навички застосування криптографічних примітивів; розуміння принципу найслабшої ланки та вміння його ідентифікувати; здатність приймати стратегічні рішення в цифрових фінансових проектах; уміння прогнозування економічних наслідків прийнятих рішень; здатність розробляти та
оцінювати вимоги до проекту; уміння обирати технології, що відповідають вимогам проекту; практичні навички опису функціональності продукту.

Формат занять

Лекції, лабораторні роботи, розрахункові завдання, консультації, самостійна робота. Підсумковий контроль – іспит.

Компетентності

ЗК 4. Здатність виявляти, ставити та вирішувати проблеми у професійній діяльності.
ЗК 5. Здатність генерувати нові ідеї (креативність) і нестандартні підходи до їхньої реалізації, гнучке адаптування до реальних професійних ситуацій, проявляти творчий підхід, ініціативу.
ЗК 11. Здатність до соціальної і професійної взаємодії та співпраці у колективі, командної роботи.
СК 3. Здатність обирати, розробляти, досліджувати та застосовувати математичні методи для розв'язання практичних задач моделювання, проектування, керування, прогнозування, прийняття рішень.
СК 7. Здатність до пошуку, вивчення та аналізу науково-технічної інформації, вітчизняного і закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження процесів та систем.
СК 13. Здатність до розробки та експлуатації спеціалізованих програмних засобів обробки великих масивів даних на основі інформаційних технологій розподілених і хмарних обчислень.

Результати навчання

РН 1. Демонструвати знання і розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці.
РН 2. Уміти формалізувати задачі, сформульовані мовою певної предметної галузі й обирати раціональний метод вирішення; розв'язувати задачі аналітичними або чисельними методами, оцінювати точність і достовірність отриманих результатів та виконувати їхню інтерпретацію.
РН 13. Знати і розуміти методи розв'язання математичних задач інтелектуального інформаційного пошуку та видобування знань.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисциплін профільного пакету ВП*.1, а саме, ВП1.1 – «Методи та технології роботи з великими даними», або ВП2.1 – «Аналіз і синтез природньомовної інформації». А також, необхідно мати знання та практичні навички з дисциплін вільного вибору (ДВВ) профільної підготовки, які викладались в першому семестрі.

Особливості дисципліни, методи та технології навчання

Інтерактивні лекції з презентаціями, «багтрекінг лекцій», лабораторні заняття із застосуванням групової динаміки, проектне навчання.

Програма навчальної дисципліни

Теми лекційних занять

1. Поняття про децентралізовані технології, їх особливості та властивості.
2. Принципи роботи блокчейну.
3. Вступ до криптографії.
4. Геш-функції.
5. Вступ до еліптичної криптографії.
6. Поняття Bitcoin.
7. Принципи роботи Bitcoin.
8. Принципи формування комісій у Bitcoin.
9. Транзакції у Bitcoin.
10. Bitcoin Script.
11. Емісія монет у Bitcoin.
12. Формати ключів у Bitcoin.
13. Дерева Меркла.
14. Процеси та ролі учасників у системі Bitcoin.
15. Децентралізовані файлообмінні системи.
16. Модель безпеки в децентралізованій обліковій системі.

Теми практичних занять

Практичні заняття не передбачені планом

Теми лабораторних робіт

Лабораторна робота 1. Механізм перевірки базових властивостей інформаційної безпеки. Створення, обробка та підтвердження транзакцій. Розв’язання класичної задачі Transaction Puzzle.
Лабораторна робота 2. Робота з HEX значеннями та варіативність перетворення. HEX <-> Int, організація бібліотеки, тестування (Python).
Лабораторна робота 3. Забезпечення базових властивостей безпеки. Алгоритми шифрування та цифрового підпису. Використання ключів та секретів великого розміру.
Лабораторна робота 4. Реалізація алгоритму гешування.
Лабораторна робота 5. Реалізація криптографічного алгоритму.
Лабораторна робота 6. Створення власного блокчейну для обраної предметної галузі. Етап технології: Terms of reference. Формуваня технічного завдання для обраного кейсу.
Лабораторна робота 7. Застосування класів KeyPair, Signature і Account.
Лабораторна робота 8. Повна побудова технологічного ланцюжка. Використання класів Operation, Transaction, Hash, Block та Blockchain.

Самостійна робота

Самостійна робота передбачає опрацювання матеріалу лекцій, розв'язування задач, підготовку до тематичного тестування в якості поточного контролю протягом семестру, виконання розрахункових робіт, підготовку до екзамену. Підсумковий контроль – екзамен.
Питання винесені на позааудиторне опрацювання.
Завдання №1: Історія виникнення та розвитку технології Blockchain та криптовалют.
Завдання №2: Цифрові гаманці та управління ключами.
Завдання №3: Реалізація блокчейну у Bitcoin.
Завдання №4: Адреси та транзакції у Bitcoin.
Завдання №5: Майнінг в Bitcoin.
Завдання №6: Чинники, що уповільнюють впровадження децентралізованих систем.

Література та навчальні матеріали

1. Блокчейн і децентралізовані системи [Текст]: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. – Харків: ПРОМАРТ, 2021. – (Distributed Lab). – ISBN 978-617-7634-40-8. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – 2021. – 458 с. : рис., табл. – Бібліогр.: с. 449-458. http://irbis-nbuv.gov.ua/cgi-bin/irbis_all/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=fullwebr&S21ALL=%28%3C.%3EK%3D%D0%91%D0%9B%D0%9E%D0%9A%D0%A7%D0%95%D0%99%D0%9D$%3C.%3E%29&Z21ID=&S21SRW=GOD&S21SRD=&S21STN=1&S21REF=10&S21CNR=20
2. Блокчейн і децентралізовані системи [Текст]: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. – Харків: ПРОМАРТ, 2021. – (Distributed Lab). – ISBN 978-617-7634-40-8. Ч. 2 / П. Кравченко [та ін.]. – 2021. – 420 с. : рис., табл. – Бібліогр.: с. 415-420. http://irbis-nbuv.gov.ua/cgi-bin/irbis_all/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=fullwebr&S21ALL=%28%3C.%3EK%3D%D0%91%D0%9B%D0%9E%D0%9A%D0%A7%D0%95%D0%99%D0%9D$%3C.%3E%29&Z21ID=&S21SRW=GOD&S21SRD=&S21STN=1&S21REF=10&S21CNR=20
3. Блокчейн і децентралізовані системи [Текст]: навч. посіб. для студентів закл. вищ. освіти : у 3 ч. – Харків : ПРОМАРТ, 2021. – (Distributed Lab). – ISBN 978-617-7634-40-8. Ч. 3 / П. Кравченко [та ін.]. – 2021. – 329 с. : рис., табл. – Бібліогр.: с. 317-329. http://irbis-nbuv.gov.ua/cgi-bin/irbis_all/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=fullwebr&S21ALL=%28%3C.%3EK%3D%D0%91%D0%9B%D0%9E%D0%9A%D0%A7%D0%95%D0%99%D0%9D$%3C.%3E%29&Z21ID=&S21SRW=GOD&S21SRD=&S21STN=1&S21REF=10&S21CNR=20
4. Kud, Aleksandr. Methodology for determining whether a blockchain token corresponds to a digital asset [Text]: methodical man. / A. A. Kud. – Kharkiv : KRPOCH, 2019. – 51 p. : tab. – Назва у вих. відом.: Методика діагностики токену блокчейну на відповідність цифровому активу / А. А. Кудь. – Бібліогр.: с. 47-50. – 5000 пр. прим. http://irbis-nbuv.gov.ua/cgi-bin/irbis_all/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=fullwebr&S21ALL=%28%3C.%3EK%3D%D0%91%D0%9B%D0%9E%D0%9A%D0%A7%D0%95%D0%99%D0%9D$%3C.%3E%29&Z21ID=&S21SRW=GOD&S21SRD=&S21STN=1&S21REF=10&S21CNR=20
5. Blockchain and accounting. Available at: https://nexia.dk.ua/blokchein-i-bukhhalterskyi-oblik [in Ukrainian, 2024].

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Студенту рекомендовано відвідувати як лекційні заняття, так і лабораторні заняття. Виконання розрахункових робіт є необхідною умовою для отримання оцінки. Виконання контрольних робіт не є обов'язковим.
Бали студента з дисципліни нараховуються за наступним співвідношенням:
– поточні тести: 20% семестрової оцінки;
– контрольні роботи: 20% семестрової оцінки;
– лабораторні роботи: 20% семестрової оцінки;
– письмові індивідуальні завдання: 20% семестрової оцінки;
– іспит: 20% семестрової оцінки.

Шкала оцінювання

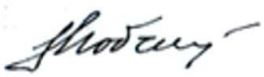
Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність.

Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	Дата погодження, підпис 31.08.2023 р.		Завідувач кафедри Олена АХІЄЗЕР
	Дата погодження, підпис 31.08.2023 р.		Гарант ОП Леонід ЛЮБЧИК