МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи
Каріна НЕМАШКАЛО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№02071211

БЛОКЧЕЙН: ОСНОВИ ТА ПРИКЛАДИ ВИКОРИСТАННЯ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**всі**
Спеціальність	**всі**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**всі**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**англійська**

Розробник:
к.т.н., доц.
підписано КЕП
Наталія ДОЛГОВА

Завідувач кафедри
кібербезпеки та
інформаційних технологій
д.т.н., проф.
Ольга СТАРКОВА

Харків
2023

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS

APPROVED
at the meeting of the department
of cybersecurity and
information technologies
Protocol № 2 of 31.08.2023.

AGREED
Vice-rector for educational and methodical work
____________ Karina NEMASHKALO

BLOCKCHAIN: BASICS AND EXAMPLES OF USE
Program of the course

Field of knowledge	**All**
Specialty	**All**
Study cycle	**first (bachelor)**
Study programme	**All**

Course status	**elective**
Language	**English**

Developer:
PhD (Engineering),
Associate Professor — digital signature ____________ Natalia Dolgova

Head of Cybersecurity and
Information Technology
Department ____________ Olga STARKOVA

Kharkiv
2023

INTRODUCTION

The relevance of the academic discipline "Blockchain: Basics and Examples of Use" and its necessity and role in training specialists is that blockchain is the latest technology that has grown in interest along with the popularity of cryptocurrencies. However, there are dozens of other ways to use blockchain apart from cryptocurrencies. Blockchain technology is considered to be the main technological breakthrough since the invention of the Internet.

The course "Blockchain: Basics and Examples of Use" is a free choice discipline (free magmaignor) for all specialties.

The purpose of teaching the discipline is to develop students' comprehensive understanding of blockchain as a technology, its key aspects and ways of applying it in economic and business contexts.

The objectives of the discipline include:

- understanding of the basic principles and mechanisms of blockchain operation,
- studying various ways of its application in the economy and business,
- development of skills in creating blockchain solutions for real business problems.

The subject of the discipline is the study of blockchain technology, including its fundamentals, such as cryptography, consensus algorithms, smart contracts, and decentralized applications. In addition, the subject includes an analysis of how blockchain can be used in various sectors of the economy, including finance, logistics, supply chain management, etc.

The object of study is blockchain systems and technologies, as well as their practical application in many areas of activity. This includes various types of blockchains (public, private, consortium), cryptocurrencies and their functioning, methods and tools for developing and implementing blockchain projects in business processes.

Learning outcomes and competencies that form the discipline are defined in Table 1.

Table 1.

Learning outcomes and competencies formed by the discipline.

Learning outcomes	**Competencies**
Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunications systems;	Ability to apply methods and means of cryptographic and technical protection of information at information facilities
Use information and communication technologies to solve socio-economic problems, prepare and present analytical reports tasks, preparation and presentation of analytical reports.	Ability to justify economic decisions based on an understanding of the laws of economic systems and processes and using modern methodological tools. Ability to effectively apply information technology in business and financial management.
Apply the acquired theoretical knowledge to solve practical problems and interpret the results in a meaningful way.	Ability to apply computer technologies and data processing software to solve economic problems, analyze information and prepare analytical reports.

COURSE CONTENT

Content Module 1. Basics of blockchain technologies

Topic 1: Decentralization in information systems.

1.1 Definition of decentralization?

The concept of decentralization for information systems. Difference between decentralized systems and redundant systems

1.2 History of decentralized systems

Decentralized file sharing systems. Decentralized data transmission systems. Decentralized computing systems. Decentralized data storage systems. Decentralized decision-making systems. Decentralized payment systems

1.3 Application of decentralization principles.

Limitations and problems of centralized systems. Application of a decentralized approach. Principles of building decentralized systems. Typical architecture of decentralized systems. Limitations of decentralized systems. Factors that slow down the implementation of decentralized systems.

Topic 2. Blockchain technology

2.1. Blockchain technology and its capabilities

Degrees of decentralization . Blockchain architecture. Blockchain properties. Application of the technology.

2.2 Differences in approaches to consensus building

Consensus building mechanism as a key element of a decentralized accounting system. Proof-of-work. Proof-of-stake. Delegated proof-of-stake. Proof-of-importance. The main criteria for classifying consensus mechanisms.

2.3 Limitations of blockchain technology and difficulties in its application

Implementation of digital identity. Digitalization of all processes. Adoption of unified data processing rules Transfer of all digital assets to one accounting system Organization of decentralized decision-making. Limitation of bandwidth. Limiting the transaction confirmation time. The problem of governance Distributed responsibility. The problem of updating the protocol

Topic 3. How Bitcoin works

3.1 History of Bitcoin

Problems that Bitcoin can solve. The main principles of Bitcoin functioning. Issuance in Bitcoin. Price formation for coins. The concept of trust in Bitcoin. Limitations of Bitcoin technology. The importance of decentralization for Bitcoin.

3.2 The use of Bitcoin.

Keys in Bitcoin. Transactions in Bitcoin. Software wallets. Hardware wallets.
Centralized storages. Backup of wallets

3.3 The concept of a Bitcoin transaction.

Bitcoin transaction. Verification of transactions. The concept of commission in Bitcoin. The concept of conflicting transactions.

3.4 The high-level architecture of Bitcoin.

The architecture of the system with blockchain technology. Processes in the Bitcoin accounting system. Roles of participants in the Bitcoin accounting system. Conditions under which consensus is achieved in Bitcoin. Consensus in Bitcoin. Comparison of Bitcoin with traditional payment systems

3.5 Confirmation of transactions in Bitcoin

Formation of transaction blocks. Requirements for new blocks. Principles of competition between users. Distribution of the block. Resolving disagreements. The concept of full transaction confirmation. Rewards for creating blocks

Topic 4. Cryptography and key management

4.1 Introduction to cryptography.

Principles of cryptographic information protection. The concept of keys. Threat and intruder model. Generation and processing of secret keys. The concept of unidirectional function and NP-complete problem. Hash function. Application of hash functions. Merkle trees. Symmetric encryption. Asymmetric cryptography.

4.2 Cryptography in Bitcoin

Features of elliptic curves. Creating Bitcoin addresses. Privacy in Bitcoin

4.3 Storage and processing of keys

approaches to wallet organization. Protecting

The main task of a digital wallet. The main

and storing the keys on the server. The keys are on the server, but only the client has access to them. Keys on the user's device. Storage of coins using multisignature. Cold, warm, and hot wallets.

Content module 2. Examples of blockchain technologies application

Topic 5. Rules for forming blocks in the blockchain.

5.1. Implementation of Blockchain in Bitcoin

Block structure. Examples of blocks in Bitcoin. Block chains.

5.2. The concept of Mempool in Bitcoin

The life cycle of the unit. Initial synchronization of the node. Checkpoints. Properties of the shared Bitcoin database

Topic 6. Blockchain rules in Bitcoin

6.1. Mining in Bitcoin

The concept and goals of mining in Bitcoin. Classification of network nodes. The concept of a resource-intensive task. Limiting the frequency of block formation. Orphan blocks. Double spend attack

6.2. Technical support of mining

Emergence and classification of special equipment for mining. Mining pools and their tasks. Mining statistics and energy consumption assessment.

Topic 7. Transactions and key formats in Bitcoin

7.1 Bitcoin transactions.

Transaction structure. Unspent Transaction Outputs (UTXOs). Receiving the rest and setting the commission. An example of a coin transfer scheme. Formation of transactions in bitcoin wallets. LockTime mechanism. Off-chain protocols. Signature hash types. Writing arbitrary data to the blockchain.

7.2. The mechanism of commissions in Bitcoin.

Data record price volatility. Solving the problem with commission volatility. Increasing the commission after sending a transaction. Segregated Witness and commissions. Option with a miner friend. Option to sell places in the confirmation queue.

7.3. Features of the Segregated Witness update

Increased throughput and backward compatibility. The Segregated Witness innovation. An example of a SegWit transaction. New concepts of transaction weight and size.

Topic 8: Blockchain, cryptocurrencies and smart contracts

8.1 Bitcoin branches and clones

Planned forks. Methods of updating software: softfork and hardfork. Unplanned softfork in Bitcoin. The concept of planned forks. Examples of planned forks in Bitcoin.

8.2 Alternative digital currencies and tokens.

Cryptocurrencies. Litecoin Dash. Difference between Litecoin, Dash, and Bitcoin mining algorithms.

BitShares. Monero . Ethereum. Cardano. Other digital currencies. Tokens.

8.3 Introduction to smart contracts.

Definition of a smart contract. The role of oracles for smart contracts. An example of a purchase in an online store. An example of a contract for a joint purchase. Classification of smart contract platforms. Difference between platforms by execution environment. Difference between platforms by the method of contract execution. Difference between platforms by the method of contract initiation.

The list of practical (seminar) and laboratory studies in the course is given in table 2.

Table 2

The list of practical (seminar) and laboratory studies

Name of the topic and/or task	Contents.
Topic 1: Task 1.	Research algorithms hashing and their use in blockchain
Topic 2. Task 2.	Working with Metamask
Topic 3. Task 3.	Working with passwords and hash values
Topic 4. Task 4.	Examination of the S-block and P-block
Topic 5. Task 5.	Working with decentralized IPFS data storage
Topics 6 - 7. Task 6.	Introduction to the process of mining and working with cryptocurrencies
Topic 8: Task 7.	Creating Ethereum smart contracts

The list of self-studies in the course is given in table 3.

Table 3

List of self-studies

Name of the topic and/or task	Content
Topic 1-8	Search, selection and review of literature on a given topic
Topic 1-8	Preparation for the Express test
Topic 1-8	Preparation for practical classes
Topic 1-8	Performing an individual task (presentation)
Topic 1-8	Preparing for the final test

The number of hours of lectures, practical (seminar) and laboratory studies and hours of self-study is given in the technological card of the course.

TEACHING METHODS

In the process of teaching a discipline, the following teaching methods are used to achieve certain learning outcomes and intensify the educational process:

Verbal (lecture-visualization (Topics 1, 2, 3, 5, 6, 7, 8), lecture-seminar (Topic 4).

Visual (demonstration (Topics 1-8)).

Practical (laboratory work (Topics 1-8)).

FORMS AND METHODS OF ASSESSMENT

The University uses a 100-point cumulative system for assessing the learning outcomes of students.

Current control is carried out during lectures, practical, laboratory and seminar classes and is aimed at checking the level of readiness of the student to perform a specific job and is evaluated by the amount of points scored: for courses with a form of semester control as grading: maximum amount is 100 points; minimum amount required is 60 points.

The final control includes current control and assessment of the student.

Semester control is carried out in the form of a semester exam or grading.

The final grade in the course is determined: for disciplines with a form of grading, the final grade is the amount of all points received during the current control.

During the teaching of the course, the following control measures are used:

Current control: performance and defense of laboratory works (7 works with 10 points each), written tests (3 works with 10 points each).

Semester control: Grading..

More detailed information on the assessment system is provided in technological card of the course.

RECOMMENDED READING

Main

1. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с.

2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.

3. Молчанов В. П. Технології розробки WEB-ресурсів [Електронний ресурс] : навч. посіб. / В. П. Молчанов, О. К. Пандорін ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (7,94 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 129 http://www.repository.hneu.edu.ua/handle/123456789/22466

4. Інформатика в сфері комунікацій [Електронний ресурс] : навч.-практ. посіб. : у 3-х ч. Ч. 3 : Використання web-технологій у сфері комунікацій / С. Г. Удовенко, В. А. Затхей, О. В. Гороховатський [та ін.] ; за заг. ред. С. Г. Удовенка; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (10.5 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. - 154 с. : іл. - Загол. з титул. екрану. - Бібліогр.: с. 153 http://repository.hneu.edu.ua/handle/123456789/24506

Additional

5. Global Bitcoin Nodes Distribution [Електронний ресурс]. – December 2018. – Режим доступу: https://bitnodes.earn.com/.

6. Накамото С. Bitcoin: A Peer-to-Peer Electronic Cash System / Сатосі Накамото. URL: https://bitcoin.org/bitcoin.pdf

7. Synergy of building cybersecurity systems: monograph / Edited by S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://repository.hneu.edu.ua/handle/123456789/25623

8. Розвиток блокчейн-бізнесу сприятиме економічному відновленню України // http://www.fin.org.ua/news/1452566[Електронний ресурс].

9. UA Крипта в Україні 2021 — гравці, закони, тенденції. URL: https://nachasi.com/crypto/2021/05/31/cryptotrends-in-ukraine/[Електронний ресурс].

10. Shmatko O. Information support for distributed teamwork knowledge management / O. Shmatko, M. Bilova. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– P. 169–192.http://repository.hneu.edu.ua/handle/123456789/24818

Information resources

11. Сайт Distributed Lab // Blockchain Experts [Електронний ресурс]. – Режим доступу: https://distributedlab.com/

12. Blockchain Explorer–Search the Blockchain | BTC | ETH [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/explorer.

13. Сайт BlockchainDemo [Електронний ресурс]. – Режим доступу: https://blockchaindemo.io/

14. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Блокчейн: основи та приклади використання" https://pns.hneu.edu.ua/enrol/index.php?id=10838