Syllabus
Course Program

BLOCKCHAIN: BASICS AND APPLICATION EXAMPLES

Specialty
113 Applied mathematics

Institute
Educational Scientific Institute of Computer Sciences and Information Technologies

Educational program
Intelligent Data Analysis

Department
Computer mathematics and data analysis

Level of education
Bachelor's level

Course type
Special (professional), Selective

Semester
7

Language of instruction
Ukrainian

Lecturers and course developers

Oksana Dubinina

Oksana.Dubinina@khpi.edu.ua
Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Professor, Professor of the Department of Computer Mathematics and Data Analysis of NTU "KhPI"

Work experience - more than 30 years. Author and co-author of more than 100 scientific and educational publications. Lecturer in the disciplines: "Higher mathematics", "Blockchain technology", "Blockchain: basics and application examples".
ORCID: https://orcid.org/0000-0002-6928-0325
h-index = 3 in Scopus – https://www.scopus.com/authid/detail.uri?authorId=57194556274
h-index = 6, i10-index = 3 in Google Scholar – https://scholar.google.com.ua/citations?user=-Qz9nSsAAAAJ&hl=ru
h-index = 1 in Publons Web of Science
https://www.webofscience.com/wos/author/record/JZD-7101-2024

More about the lecturer on the department's website

General information

Summary

The course covers the main technical and fundamental aspects of blockchain technology and application levels, providing master's level students with an opportunity to deeply understand the basics. The course is distinctive in that the material is presented at the intersection of the principles of operation, benefits and risks of innovative information technologies. The course includes two content modules. Mastering the discipline involves the formation of modern engineering thinking, training in the basic technological tools necessary for research, analysis and modelling of processes in the search for optimal solutions and the selection of the best means of implementing these solutions, methods of research and solving mathematically formalised problems, the ability to analyse and synthesise the results and input data.

Course objectives and goals

Acquiring the competencies necessary for further work by mastering the technical details of the functioning of blockchain mechanisms, learning new concepts related to the decentralised technology stack, developing students' logical and algorithmic thinking; mastering the methods of research and analysis of applied and engineering tasks. As a result of mastering the discipline, students develop the following skills: the ability to understand security services and how to provide them; skills in applying cryptographic primitives; understanding the principle of the weakest link and the ability to identify it; the ability to make strategic decisions in digital financial projects; the ability to predict the economic consequences of decisions; the ability to develop and evaluate project requirements; the ability to choose technologies that meet project requirements; practical skills in describing product functionality.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control in the form of an exam.

Competencies

GC 2. Ability to apply knowledge in practical situations.
GC 3. Ability to generate new ideas (creativity).
GC 5. Ability to conduct research at the appropriate level.
GC 6. Ability to abstract thinking, analysis and synthesis.
GC 7. Ability to search, process and analyse information from a variety of sources.
GC 9. Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity)
SC 2. Ability to perform tasks formulated in mathematical form.
SC 14. Ability to understand the task formulated in the language of a particular subject area, to search and collect the necessary initial data.
SC 20. Ability to develop and operate software tools for intellectual analysis of measurement and observation data, texts, signals and images.

Learning outcomes

LO 3. Formalise problems formulated in the language of a particular subject area; formulate their mathematical formulation and choose a rational method of solution; solve the obtained problems by analytical and numerical methods, evaluate the accuracy and reliability of the results.
LO 11. Be able to apply modern technologies of programming and software development, software implementation of numerical and symbolic algorithms.
LO 15. To be able to organise their own activities and get results within a limited time.
LO 22. To know and understand the methods of solving mathematical problems of intellectual information retrieval and knowledge extraction.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures – 16 hours, laboratory classes – 32 hours, self-study – 72 hours.

Course prerequisites

‘Mathematical Analysis, Linear Algebra, Fundamentals of Cybersecurity, Information Security Management, Algorithmisation and Programming, Databases and Information Systems.

Features of the course, teaching and learning methods, and technologies

Interactive lectures with presentations, ‘bugtracking lectures’, laboratory classes with the use of group dynamics, project-based learning.

Program of the course

Topics of the lectures

1. Decentralisation in information systems.
2. Principles of blockchain operation.
3. Introduction to cryptography and key management.
4. Hash functions.
5. Introduction to elliptic cryptography.
6. The concept of Bitcoin.
7. Principles of Bitcoin operation.
8. Principles of commission formation in Bitcoin.
9. Transactions in Bitcoin.
10. Bitcoin Script.
11. Issue of coins in Bitcoin.
12. Key formats in Bitcoin.
13. Merkle trees.
14. Processes and roles of participants in the Bitcoin system.
15. Decentralised file sharing systems.
16. Security model in a decentralised accounting system.

Topics of the workshops

Practical training is not included in the plan.

Topics of the laboratory classes

Laboratory work 1, 2. Mechanism for checking the basic properties of information security. Creating, processing and confirming transactions. Solving the classic Transaction Puzzle problem.
Laboratory work 3, 4. Working with HEX values and conversion variability. HEX <-> Int, library organisation, testing (Python).
Laboratory work 5, 6. Providing basic security properties. Encryption and digital signature algorithms. Use of keys and secrets of large size.
Laboratory work 7, 8. Implementation of the hashing algorithm.
Laboratory work 9, 10. Implementation of a cryptographic algorithm.
Laboratory work 11, 12. Creating your own blockchain for the selected subject area. Technology stage: Terms of reference. Formation of terms of reference for the selected case.
Laboratory work 13, 14. Application of the KeyPair, Signature and Account classes.
Laboratory work 15, 16. Complete construction of the technological chain. Using the Operation, Transaction, Hash, Block and Blockchain classes.

Self-study

Independent work involves studying lecture material, solving problems, preparing for thematic testing as a current control during the semester, performing calculations, and preparing for the exam. The final control is an exam.

Questions are submitted for extracurricular study.

Task #1: History of the emergence and development of Blockchain technology and cryptocurrencies.
Task #2: Digital wallets and key management.
Task #3: Implementation of the blockchain in Bitcoin.
Task #4: Addresses and transactions in Bitcoin.
Task #5: Mining in Bitcoin.
Task #6: Factors that slow down the implementation of decentralised systems.

Non-formal education

In the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent professional courses/trainings, civic education, online education, professional internships, etc.

In particular, certain topics of this component, namely:
1. The concept of decentralised technologies, their features and properties.
2. Principles of blockchain operation.
3. Introduction to cryptography.
4. Hash functions.
5. Introduction to elliptic cryptography.
6. The concept of Bitcoin.
7. Principles of Bitcoin operation.
8. Principles of commission formation in Bitcoin.
9. Transactions in Bitcoin.
10. Bitcoin Script.
can be taken into account in case of successful completion of the course 'Blockchain and decentralised technologies', 45 hours / 1.5 ECTS, duration: 3 months,
https://distributed.education/blockchain-course

Course materials and recommended reading

Basic literature

1. Blockchain and decentralized systems. Authors' edition in three volumes . Vol . 1 / P. Kravchenko , B. Skriabin , O. Dubinina . – Kyiv : 24 Print, 2024. – 446 p.: 191 figures, 11 tables.
ISBN 978-6-1776-3427-9
ISBN 978-6-1776-3428-6 (vol. 1)
2. Blockchain and decentralized systems : in three volumes. V.2 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kyiv : 24 Print, 2024. – 396 p. : 256 figures; 17 tables; references: 78 titles.
ISBN 978-617-7634-27-9
ISBN 978-617-7634-72-9 (v.2)
3. Blockchain and decentralized systems : in three volumes. V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina, S. Kozlov. – Kyiv : 24 Print, 2024. 344 p.: 185 figures; 3 tables; references: 204 titles.
ISBN 978-617-7634-27-9
ISBN 978-617-7634-79-8 (v. 3)

Additional literature

4. Kud, Aleksandr. Methodology for determining whether a blockchain token corresponds to a digital asset [Text]: methodical man. A. Kud. - Kharkiv: KRPOCH, 2019. - 51 p.: tab. - Title in the original language: Methodology for diagnosing a blockchain token for compliance with a digital asset /A. A. Kud. - 5000 copies.
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 technologies and cryptocurrencies: risks and cybersecurity: SIDCON, 2022. 316 p. - ISBN 978-617-95100-7-6.
https://www.yakaboo.ua/ua/tehnologii-blokchejn-ta-kriptovaljuta-riziki-ta-kiberbezpeka.html].

Internet resources

6.
https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Students are encouraged to attend both lectures and laboratory classes. Completion of calculations is a prerequisite for obtaining a grade. Tests are compulsory.
The student's points in the discipline are calculated according to the following ratio:
- current tests: 20% of the semester grade;
- control works: 20% of the semester grade;
- laboratory work: 20% of the semester grade;
- written individual assignments: 20% of the semester mark;
- exam: 20% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU «KhPI»: to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU «KhPI» are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by

Date, signature
29.08.2024

Head of the Department
Olena AKHIIEZER

Date, signature
29.08.2024

Guarantor of the Educational Program
Olena AKHIIEZER