MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS

"APPRUVED"
Deputy Director
(Vice-Rector of Educational research)

M. V. Afanasyev

BLOCKCHAIN: FUNDAMENTALS AND EXAMPLES OF USE

steering document of the academic discipline

Area of expertise	**All areas**
Speciality	**All specialities**
Grade level	**The first (Bachelor's)**
Academic Program	**All academic programs**

Type of discipline	**selective**
Teaching, studying and evaluating language	**English**

Head of *Cybersecurity and Information Technology* Department — Yevseiev S.P.

Kharkiv
S. Kuznets KhNUE
2018

APPRUVED

At the session of the Cybersecurity and Information Technology Department
Protocol # 5 from 1.11.2018.

Drafters::
Shmatko O.V., Ph.D, Associate Professor Senior Lecturer of Department CIT,
Lebid O.V., Ph.D, Associate Professor Senior Lecturer of Banking Department

The list of renewal and re-approval of academic discipline program

Academic year	Data of the session of the Department – Drafter of SDAD	Protocol Number	Signature of Head of Department
2018/2019			

1. Introduction

Annotation for the academic discipline:

The rapid development of information technology, the hybrid of modern cyber threats and vulnerabilities, and the inability of traditional cryptosystems to withstand cyber-attacks of the fifth generation require the use of new approaches to the establishing of a secure business process. One of these approaches is rapidly expanding in various sectors of society - the establishing of decentralized systems based on blockschain technologies. The core idea is in peer-to-peer privileges for all users of such systems basing on the cryptographic protocols of the digital signature of those heats. These advantages, as well as others properties of blockchain technologies provide their distribution and rapid expansion of decentralized systems using cryptographic.

The discipline "Currency, Cryptography and Blockchain Technologies" is a free-chosen academic discipline (a free-chosen Minor) for all specialities. It is studied in the second semester of Master's Degree Program in the size of 150 hours (5 credits ECTS), The course provides two content modules and two modular tests. The discipline ends up with an offset.

The Object of the academic discipline is a blockchain technology and other activity related to it.

The Subject of the academic discipline are theoretical concepts, principles of operation and application of blockchain technologies.

The Purpose of the academic discipline:

is establishing of the theoretical basis for future Bachelors in skills of using of blockchain technologies, economic relations based on crypto-currency and smart contracts.

The main objectives in studying the academic discipline are:

to learn the principles and rules for the use of cryptographic tools in blokchain technologies;

to learn the methodological foundations of the development and operation of blockchain platforms;

to acquire realization abilities for use of cryptography and the functioning of smart contracts;

to acquire effective means of limiting the risks of creating and using crypto-currency, using smart contracts.

Course	**3**	
Semester	**5**	
Number of ECTS credits	**5**	
Audit lessons	**lectures**	**32**
	laboratory	**32**
Independent work		**86**
Form of final control	**offset**	

2. Competence and results of studying a discipline:

Competence	Learning outcomes
The ability to use information and communication technologies in order to find new information, create databases, analyze distributed circuits, communication channels, process control systems, databases, operational planning of systems based on analysis of information flows and their optimization.	Design future professional activities, taking into account its importance for the citizen and the government, as well as directions of information and cyber security development. To carry out professional activity on the basis of knowledge of modern information and communication technologies. Apply software, skills in telecommunication and computer networks. Use specialized computer programs in professional activities. Choose the appropriate programming technology, perform a task specification analysis. Perform software analysis to find, identify, identify, and eliminate programming errors
The ability to solve specialized tasks and practical problems concerning the use of blockchain technology in various branches of the economy.	Using of crypto currency within the current legal field. Being able to use different platforms based on technology blockade in business processes. Using smart contracts, track their execution. Planing and predicting the use of blockchain technology in various spheres of life.

3. Program of the discipline

The content module 1. Fundamentals of cryptographic methods in the blockchain technology

Topic 1. Trust and vulnerability.
1.1. A brief history of scaling a human trust.
1.2. Society of high and low trust.
1.3. Types of Trust Model: Peer-to-Peer, Leviathan and Broker.

Topic 2. Basics of cryptography
2.1. Basics of cryptography.
2.2. Basics of cryptosystems of traditional cryptography.
2.3. Basics of public key cryptosystems.
2.4. Basics of Digital Signature. Hash functions.

Topic 3. Using of cryptography in blockchain
3.1. Fundamentals of decentralized systems.
3.2. Use of hash functions in blockschain technologies.
3.3. Digital signatures for signing transactions.

Topic 4. Blockchain technology, its capabilities and limitations

4.1. The maintenance of the blockade technology. Hash Merkle tree.Special transaction types Hard & soft fork.

4.2. The limitation of the blockchain technology, its types (public and private).

4.3. Differences in approaches to reaching consensus.

4.4. Principles of system security analysis.

The content module 1. Specifics and examples of using blockchain technology

Topic 5. Implementation of blockchain in bitcoin

5.1. History of occurrence and stages of establishing of bitcoin.

5.2. Bitcoin as a payment system.

5.3. The economy of bitcoin: specifics of use at the present stage.

Topic 6. Blockchain as a platform

6.1. Secure stamp of time: specifics of use and implementation.

6.2. Practical application of the bitcoin properties: the organization and conduct of lotteries, tickets, colored coins.

6.3. The essence of the market forecasts and analysis of the possibility of its construction on the basis of bitcoin.

Topic 7. Smart Contracts

7.1. Fundamentals of contractual law. Smart Contracts and their capacity.

7.2. Trust in algorithms, impact on society. How can existing legal systems be integrated? OpenZeplin, OpenLaw. 10/9 12

7.3. Writing of reasonable contracts. Colored tokens, Cryptokitties, Solidity, and Chaincode.

Topic 8. Non-financial examples of the use of blockchain technology

8.1. Copyright protection, digital assets and tokenization.

8.2. The Internet of Things and the use of the blockchain technology in it.

8.3. Electronic voting

4. The procedure of evaluation of the learning results

The system of evaluation of the developed competencies of students takes into account the types of occupations, which according to the curriculum program include lectures, seminars, practical classes, as well as independent work. Assessment of the developed competencies in students is carried out using a 100-point accumulation system. In accordance with the Provisional Regulations "On the Procedure for Assessing the Results of Students' Learning Based on the Accumulated Bulletin-Rating System" S. Kuznets KhNEU, control measures include:

Current control over the semester during lectures and laboratory classes and is estimated by the sum of the points scored (the maximum amount is 60 points; the minimum amount that allows the student to take the exam - 35 points);

modular control carried out in the form of a colloquium as an intermediate mini-exam on the initiative of the teacher, taking into account the current control over the relevant content module and aims to integrate the evaluation of the student's learning outcomes after studying the material from the logically completed part of the discipline - content module;

final / semester control, conducted in the form of a credit, according to the schedule of the educational process.

The procedure for carrying out the current assessment of students' knowledge. Assessment of students' knowledge during lecture and laboratory classes and fulfillment of individual tasks is carried out according to the following criteria:

understanding, degree of assimilation of the theory and methodology of the problems under consideration; the degree of assimilation of the actual material of the discipline; acquaintance with the recommended literature, as well as contemporary literature on the issues under consideration; the ability to combine theory with practice when considering production situations, solving tasks, performing calculations in the process of performing individual tasks and tasks submitted for consideration in an audience; logic, structure, style of presentation of the material in written works and speeches in the audience, ability to substantiate their position, to generalize information and to draw conclusions; arithmetic correctness of the implementation of an individual and complex settlement task; the ability to conduct a critical and independent assessment of certain problem issues; the ability to explain alternative views and the presence of their own point of view, position on a particular problem issue; application of analytical approaches; quality and clarity of reasoning; logic, structuring and substantiation of conclusions on a specific problem; independence of work; literacy of presentation of the material; use of comparison methods, generalizations of concepts and phenomena; registration of work.

The general criteria for evaluating non-auditing independent work of students are: the depth and strength of knowledge, the level of thinking, the ability to systematize knowledge on specific topics, the ability to make sound conclusions, the possession of categorical apparatus, skills and techniques of performing practical tasks, the ability to find the necessary information, carry out its systematization and processing, self-realization on practical and seminars.

The final control of the knowledge and competences of students in the discipline is based on a score that is considered to be successful if the student scored 60 points or more during the semester.

A student should be **considered certified** if the sum of the points obtained on the basis of the results of the final / semester test of success is equal to or exceeds 60.

The final score in the discipline is calculated on the basis of the points obtained during the exam and the points obtained during the current control over the accumulation system. The total score in the points for a semester is: "60 and more points -" enrolled "," 59

and less points - not taken into account "and entered in the" Record of success "of the academic discipline.

Distribution of points by weeks

Topics of the content module			Lecture classes	Laboratory classes	Checking the essay	Presentation	Express-quiz	Testing	Written control work	Colloquium	Total
Content module	Topic	Week									
1	2	3	4	5	6	7	8	9	10	11	12
Content module 1.	1	1	1	1			1				3
		2	1	4			1				6
	2	3	1	1			1				3
		4	1	4			1				6
	3	5	1	1			1				3
		6	1	4			1				6
	4	7	1	1			1				3
		8	1	4			1		11		17
1	2	3	4	5	6	7	8	9	10	11	12
Content module 2.	5	9	1	1			1				3
		10	1	3			1				5
	6	11	1	1			1				3
		12	1	3			1				5
	7	13	1	1	10		1				13
		14	1	3			1		11		16
	8	15	1	1			1				3
		16	1	3			1				5
	offset										
Total			16	36	10		16		22		100

Scale: national and ECTS

The amount of points for all types of educational activities	Rating ECTS	Score on a national scale	
		for exam, course project (work), practice	for the offset
90 – 100	A	perfectly	Accepted
82 – 89	B	well	
74 – 81	C		
64 – 73	D	satisfactorily	
60 – 63	E		
35 – 59	FX	unsatisfactorily	not accepted
1 – 34	F		

5. Recommended Books

5.1 Main

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6
2. Кравченко П. Блокчейн и децентрализованные системы: учебн. пособие для студ. заведений вісш. образования: в 3 частях. Ч.1/ П.Кравченко, Б. Скрябин, О. Дубинина, – Харьков: ПРОМАРТ, 2018. – 400 с.
3. Агеев А. И. Криптовалюты, рынки и институты / А. И. Агеев, Е. Л. Логинов // Экономические стратегии. – 2018. – № 1. – С. 94–107.
4. Андрюшин С. А. Открытый банкинг, кредитная активность, регулирование и надзор // Банковское дело. – 2017. – № 6. – С. 26–34.
5. Бауэр В. П. Блокчейн как основа формирования дополненной реальности в цифровой экономике /В. П. Бауэр, С. Н. Сильвестров, П. Ю. Барышников // Информационное общество. – 2017. – № 3. – С. 30–40.
6. Блокчейн и децентрализованные системы : учеб. Пособие для студ. Заведений высш.образования : в 3 частях. Ч.1 / П. Кравченко, Б. Скрябин, О. Дубинина. – Харьков : ПРОМАРТ, 2018. – 408 с.
7. Ведута Е. Цифровая экономика приведет к экономической киберсистеме // Международная жизнь. – 2017. – № 10. – С. 87–102.
8. Генкин А. С. Криптотехнологии и криминальные риски: есть ли повод для тревоги? // Страховое дело. – 2017. – № 5. – С. 47–55.

5.2 Additional

9. Coindesk, What can you buy with Bitcoin, 2015.
10. L. Kehoe, D. Daltion, C. Lonowicz, T. Jankovich, Blockchain Disruptingthe Financial Services Industry?, 2015.
11. Shelkovnikov, Blockchain Enigma. Paradox. Opportunity, 2016.
12. M. Morisse, Cryptocurrencies and Bitcoin: Charting the Research Land-scape, in: Americas Conference on Information Systems, pp. 1–16.
13. F. Reid, M. Harrigan, An analysis of anonymity in the bitcoin system,Security and Privacy in Social Networks (2013) 197–223.
14. Eyal, E. G. Sirer, Majority is not Enough: Bitcoin Mining is Vulner-able, 2013.
15. G. O. Karame, E. Androulaki, S. Capkun, Double-spending fast pay-ments in bitcoin, Proceedings of the 2012 ACM conference on Computerand communications security. (2012).
16. F. Glaser, L. Bezzenberger, Beyond Cryptocurrencies - A Taxonomy ofDecentralized Consensus Systems, in: European Conference on Infor-mation Systems, 57, pp. 1–18.

5.3 Information resources of the Internet

17. www.coindesk.com/information/applications-use-cases-blockchains/
18. https://www.nasdaq.com/article/4-innovative-use-cases-for-blockchain-cm901636
19. Starting 16 minutes: https://www.youtube.com/watch?v=cHe_ow9v094
20. https://blockchain.hneu.edu.ua/