Zał. nr 5 do ZW 16/2020

Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Blockchain i kryptowaluty**
Name of the course in english	:	**Blockchain and cryptocurrencies**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4118G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	90		90		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3		3		
including the number of points corresponding to the classes of practical (P)			3		
including the number of points corresponding occupations requiring direct contact (BK)	2		2		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Gaining knowledge on the technical mechanisms of cryptocurrencies, blockchain, smart contracts; learning skill for designing and implementation of secure systems based on these technologies

C2 ability to programme and analyse smart-contracts

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 understanding cryptographic and distributed systems background of blockchain, cryptocurrencies and smart contracts

W2 awareness of the level of security and reliability of the mechanisms being the subject of the lecture

W3 knowledge of the basics of smart contracts and methods of their implementation

The student skills:

U1 ability to implement a smart contract

U2 ability to evalate threats and security guarantees of systems based on the technologies in question

U3 the ability to use blockchain technology to build secure data repositories

The student's social competence:

K1 can determine pragmatic applications of the discussed technologies in the context of financial trading

K2 is able to correctly assess the sociological and psychological context of solutions

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to cryptocurrencies	4h
Wy2	Consensus. Models, attacks. Nakamoto Consensus	4h
Wy3	Proof of work	2h
Wy4	Proof of space	2h
Wy5	Verifiable delay functions	2h
Wy6	Proof of stake	2h
Wy7	Privacy and mixing	2h
Wy8	zk-SNARKs	4h
Wy9	Smart-contract security	4h
Wy10	Ethereum	2h
Wy11	zCash	2h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	Managing wallets	2h
Lab2	Hands on with Ethereum	2h
Lab3	Smart contracts	2h
Lab4	ERC20 tokens and ICOs	2h
Lab5	Merkle trees	2h
Lab6	Ethereum attacks	2h
Lab7	zk-SNARKs	4h
Lab8	Mix-servers	4h
Lab9	Solidity	10h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K2	Exam
F2	U1-U3, K1-K2	Problem sets and final project
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. Bitcoin’s Academic Pedigree - Arvind Narayanan, Jeremy Clark
2. Bitcoin: A Peer-to-Peer Electronic Cash System - Satoshi Nakamoto
3. Foundations of Distributed Consensus and Blockchains - Elaine Shi
4. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER - DR. GAVIN WOOD
5. Solidity - https://docs.soliditylang.org/en/latest/
6. Zerocash: Decentralized Anonymous Payments from Bitcoin - Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza

SUPERVISOR OF COURSE

dr Filip Zagórski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Blockchain i kryptowaluty
WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
W1	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W09	C1	Wy1-Wy11	1 2 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08 K2_W09	C1	Wy1-Wy11	1 2 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08 K2_W09	C1	Wy1-Wy11	1 2 6
U1	K2_U01 K2_U05 K2_U06 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
U3	K2_U03 K2_U05 K2_U06 K2_U07 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy11 Lab1-Lab9	1 2 3 4 5 6
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy11 Lab1-Lab9	1 2 3 4 5 6