POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

COURSE DESCRIPTION CARD - SYLLABUS

Course name
Blockchain Technology and Quantum Computations [S2Inf1E-CYB>BTQ]

Course

Field of study	Year/Semester
Computing	1/1
Area of study (specialization)	Profile of study
Cybersecurity	general academic
Level of study	Course offered in
second-cycle	English
Form of study	Requirements
full-time	compulsory

Number of hours

Lecture	Laboratory classes	Other
15	15	0
Tutorials	Projects/seminars	
0	0	

Number of credit points

2,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Lecturers

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

mgr inż. Oskar Niżnik
oskar.niznik@put.poznan.pl

Prerequisites

A student beginning this course should have an in-depth knowledge of cryptography.

Course objective

As part of the course, students will learn about blockchain technology, the concept of a decentralized database, cryptocurrencies - both technical and economic-legal aspects. They will learn about applications of blockchain technology. The second part of the lectures and exercises will cover quantum computing, theoretical foundations, the threats of quantum computers and post-quantum algorithms.

Course-related learning outcomes

Knowledge:
the student has detailed knowledge of:
- structure of blockchains, cryptographic mechanisms used and security of this technology
- attacks on the blockchain structure and the possibilities and limitations of their use

- theoretical basic knowledge about quantum cryptography and post-quantum algorithms
- threats and possibilities of quantum cryptography.

Skills:
the student is able to:
- design a blockchain structure, use it in a specific application
- identify the dangers of quantum cryptography and identify research directions for post-quantum algorithms.

Social competences:
the student understands:
- how important it is to carefully select the components from which a blockchain, smart contract is built
- the importance of implementation, as improper implementation may reduce the security level of the entire system.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Knowledge acquired during the lecture is verified during the 45-minute written test on the last class, consisting of 4 questions. The credit threshold: more than 50% of the points. Issues on which the questions are based are available on eKursy platform.
The skills acquired in the laboratory are verified on an ongoing basis in subsequent classes, during which students carry out the subsequent stages of the exercise/implementation. It is allowed to work in 2-person teams.

Programme content

Course Content:
Blockchain Technology, Cryptocurrencies, Smart Contracts
Quantum Computing. Post-Quantum Algorithms

Course topics

Lecture:
1. Introduction to blockchain technology and cryptocurrencies, the concept of decentralization.
2. Algorithms used in blockchain technology - security and limitations
3. Platforms used in implementations - examples of applications
5. Smart contracts - concept and applications
6. Introduction to quantum computations, threats and possibilities
7. Post-quantum algorithms.
Laboratory:
Laboratory exercises are performed by each student individually or in pairs. Different tasks and projects are assigned, which implement in practice, step by step, the content presented in the lecture.

Teaching methods

The lecture is conducted in an interactive manner (with the formulation of questions to students) using multimedia presentations. Materials are made available to students in electronic version.
Laboratory exercises are performed by each student individually or in pairs, different tasks are assigned. The teacher supervises and consults subsequent stages of implementation. Depending on the pace of students" work, further tasks are assigned.

Bibliography

Basic
1. Dhillon V., Metcalf D., Hooper M., Zastosowania technologii Blockchain, PWN, 2018
2. Song J., Zrozumieć Bitcoin. Programowanie kryptowalut od podstaw, Helion, 2020
Additional
1. Ward Beullens, Jan-Piete D'Anvers, Andreas HÅNulsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, and Nigel P. Smart. Post-quantum cryptography - current state and quantum mitigation, 2022.

2. https://www.enisa.europa.eu/publications/
post-quantum-cryptography-current-state-and-quantum-mitigation.

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	30	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	20	1,00