



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Technologia Blockchain i obliczenia kwantowe [S2Inf1E-CYB>BTQ]

Przedmiot

Kierunek studiów

Informatyka/Computing

Rok/Semestr

1/1

Studia w zakresie (specjalność)

Cyberbezpieczeństwo

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

angielski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

15

Laboratorium

15

Inne

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Anna Grocholewska-Czuryło

anna.grocholewska-czurylo@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć pogłębioną wiedzę w zakresie kryptografii.

Cel przedmiotu

W ramach przedmiotu studenci zapoznają się z technologią blockchain, koncepcją zdecentralizowanej bazy danych, kryptowalutami - zarówno aspektami technicznymi jak i ekonomiczno-prawnymi. Poznają zastosowania technologii blockchain. Druga część wykładów i ćwiczeń obejmować będzie obliczenia kwantowe, podstawy teoretyczne, zagrożenia związane z kwantowymi komputerami oraz algorytmy post-quantowe

Przedmiotowe efekty uczenia się

Wiedza:

student/ka ma szczegółową wiedzę na temat:

- budowy blockchainów, wykorzystywanych mechanizmów kryptograficznych i bezpieczeństwa tej technologii
- ataków na strukturę blockchainów oraz możliwości i ograniczeń do stosowania
- teoretyczne podstawy kryptografii kwantowej i algorytmów post-quantowych

- zagrożenia i możliwości związane z kryptografią kwantową

Umiejętności:

student/ka potrafi:

- zaprojektować strukturę blockchained, wykorzystać ją w konkretnym zastosowaniu
- zaprojektować i zaimplementować inteligentne kontrakty dla różnych przykładów biznesowych aplikacji
- wskazać zagrożenia związane z kryptografią kwantową oraz wskazać kierunki badań algorytmów post-kwantowych

Kompetencje społeczne:

student/ka rozumie:

- jak ważne jest staranne dobieranie komponentów z których zbudowany jest blockchain, inteligentny kontrakt
- jak ważna jest implementacja, gdyż niewłaściwa może obniżyć poziom bezpieczeństwa całego systemu.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu weryfikowana jest podczas pisemnego 45-minutowego kolokwium na ostatnich zajęciach, składającego się z 4 pytań. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania są dostępne na platformie eKursy. Umiejętności nabyte na laboratorium, weryfikowane są na bieżąco na kolejnych zajęciach, na których studenci przeprowadzają kolejne etapy ćwiczenia/implementacji. Dopuszcza się pracę w zespołach 2-osobowych.

Treści programowe

Treści programowe:

Technologia blockchain, kryptowaluty. Inteligentne kontrakty
Obliczenia kwantowe. Algorytmy post-kwantowe

Tematyka zajęć

Wykład:

1. Wprowadzenie do technologii blockchain i kryptowalut, koncepcja decentralizacji.
2. Algorytmy wykorzystywane w technologii blockchain - bezpieczeństwo i ograniczenia
3. Platformy wykorzystywane w implementacjach - przykłady zastosowań
5. Inteligentne kontrakty - koncepcja i zastosowania
6. Wprowadzenie do tematyki komputerów kwantowych, zagrożeń i możliwości
7. Algorytmy post-kwantowe

Laboratorium:

Cwiczenia laboratoryjne każdy student wykonuje indywidualnie lub w parach, przydzielone zostają różne zadania i projekty, które krok po kroku implementują w praktyce treści przedstawiane na wykładzie.

Metody dydaktyczne

Wykład prowadzony jest w sposób interaktywny (z formułowaniem pytań do studentów) przy użyciu prezentacji multimedialnych. Materiały udostępniane są studentom w wersji elektronicznej.

Cwiczenia laboratoryjne każdy student wykonuje indywidualnie lub w parach. Przydzielone zostają różne zadania. Prowadzący nadzoruje i konsultuje kolejne etapy implemetacji. W zależności od tempa pracy studentów zadawane są kolejne zadania.

Literatura

Podstawowa

1. Dhillon V., Metcalf D., Hooper M., Zastosowania technologii Blockchain, PWN, 2018.
2. Song J., Zrozumieć Bitcoin. Programowanie kryptowalut od podstaw, Helion, 2020.

Uzupełniająca

1. Ward Beullens, Jan-Pieter 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>.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	20	1,00