Poznan University of Technology

Blockchain Technology And Quantum Computation Introduction

Jakub Piotr Hamerliński

Blockchain Technology And Quantum Computation
Introduction - Agenda

01. About me
02. Subject overview
03. Subject plan
04. Course completion rules
05. Project requirements
06. Sources
07. Contact and Q&A
08. Tasks

About me

About me

My name is Jakub Piotr Hamerliński, M.Eng. I'm a DevOps engineer passionate about cybersecurity and cryptography.

Pronouns: he/him/his.

My GitHub
https://github.com/hamerlinski

My LinkedIn
https://www.linkedin.com/in/hamerlinski

Subject overview

Subject overview

Blockchain Technology And Quantum Computation

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.

Subject plan

Blockchain Technology And Quantum Computation

Week 1:

01. Introduction to the course and overview of the topics to be covered
02. Definition and characteristics of blockchain technology
03. Cryptography fundamentals: encryption, decryption, hash functions, digital signatures
04. Types of blockchains: public, private, and consortium
05. Examples of blockchain-based applications

Card subject to change

Subject plan

Blockchain Technology And Quantum Computation

Week 2:

01. Cryptographic mechanisms used in blockchain technology: proof-of-work, proof-of-stake, Byzantine fault tolerance
02. Smart contracts and their role in blockchain-based applications
03. Designing a blockchain structure for a specific application
04. Hash functions and digital signatures in blockchain technology
05. Secure multi-party computation

Card subject to change

Subject plan

Blockchain Technology And Quantum Computation

Week 3:

01. Security aspects of blockchain technology: attacks on the blockchain structure,
02. 51% attack, double-spend attack, selfish mining, and sybil attack
03. Eclipse attack and routing attacks
04. Spam and phishing attacks
05. Cryptocurrency fundamentals: Bitcoin, Ethereum, Litecoin
06. Economic and legal aspects of cryptocurrencies

Card subject to change

Subject plan

Blockchain Technology And Quantum Computation

Week 4:

01. Introduction to quantum computing: quantum bits, quantum gates, quantum circuits
02. Theoretical foundations of quantum cryptography: BB84 protocol, E91 protocol
03. Limitations of classical cryptography and the need for quantum cryptography
04. Quantum algorithms, including Shor's algorithm and Grover's algorithm
05. Quantum attacks on blockchain technology

Card subject to change

Subject plan

Blockchain Technology And Quantum Computation

Week 5:

01. The threats of quantum computing to current cryptographic mechanisms
02. Post-quantum cryptographic mechanisms, including lattice-based cryptography, hash-based cryptography, and code-based cryptography
03. Research directions for post-quantum cryptography
04. Possibilities of quantum cryptography: quantum key distribution, quantum coin tossing
05. Practical implementation of quantum cryptography
06. Quantum-resistant blockchain algorithms and their implementation

Card subject to change

Subject plan

Blockchain Technology And Quantum Computation

Week 6:

01. Students will present their final projects, which should demonstrate their understanding and application of blockchain technology and quantum computations.
02. The presentations will be evaluated based on the quality of the project, the demonstration of knowledge and skills, and the ability to answer questions and engage in discussion

Card subject to change

Course completion rules

Course completion rules

Blockchain Technology And Quantum Computation

01. Exercises during classes and work in the classroom + tests/quiz.
02. Project.

Lessons typically will start with topic introduction. Then students will perform small and simple tasks which will be reviewed and graded before end of class.

$$\mathbb{X} = 0.3 \times \mathbb{E} + 0.7 \times \mathbb{P}$$

$\texttt{where } \mathbb{E} \texttt{ means average from excercies},$
$\texttt{and } \mathbb{P} \texttt{ means grade from the project}$

Each of the components of the grade must be positive.

Course completion rules

Blockchain Technology And Quantum Computation

1 absences from classes allowed. Each subsequent one must be made up.

Project requirements

Blockchain Technology And Quantum Computation

Simple Blockchain Implementation
Objective: The objective of this project is to implement a basic blockchain structure that can be used to store and verify transactions. The blockchain should include the necessary components such as blocks, transactions, and cryptographic mechanisms to ensure data integrity and security.

Projects can be done alone or in groups of 2.

Project requirements

Blockchain Technology And Quantum Computation

Requirements:

01. The blockchain should be implemented using a programming language of your choice - no restrictions.
02. The blockchain should support the addition of new blocks containing transaction data, which should be stored securely.
03. The blockchain should use cryptographic mechanisms such as hashing and digital signatures to ensure the integrity and security of the data. Cryptographic mechanisms such as hashing can be achieved with external libraries like OpenSSL.
04. The blockchain should support consensus mechanisms such as proof-of-work or proof-of-stake to ensure the validity of the blocks.

Project requirements

Blockchain Technology And Quantum Computation

Requirements:
05. The blockchain should include a simple user interface to allow users to add and view transactions, and to view the current state of the blockchain.

06. The blockchain should include basic security features such as authentication and access control to prevent unauthorized access to the blockchain.

07. The blockchain should be tested and evaluated for its performance and security.

Project requirements

Blockchain Technology And Quantum Computation

Deliverables:

01. Source code for the blockchain implementation.
02. A report, written using LaTeX, describing the implementation, including design decisions, implementation details, and test results.
03. A short, 5 minutes, demonstration of the blockchain implementation, including adding transactions, verifying blocks, and viewing the blockchain state.

All of above should be comitted to public repository before last meeting.

Project requirements

Blockchain Technology And Quantum Computation

Evaluation: The project will be evaluated based on the following criteria:

01. Completeness and correctness of the implementation.
02. Use of cryptographic mechanisms to ensure data integrity and security.
03. Use of consensus mechanisms to ensure the validity of the blocks.
04. User interface design and usability.
05. Security features and measures to prevent unauthorized access.
06. Performance and scalability of the blockchain implementation.
07. Quality and clarity of the report and demonstration.

Project will be presented on the last meeting.

Sources

01. Dhillon V., Metcalf D., Hooper M., Zastosowania technologii Blockchain, PWN, 2018
02. Song J., Zrozumieć Bitcoin. Programowanie kryptowalut od podstaw, Helion, 2020
03. Ward Beullens, Jan-Piete D'Anvers, Andreas HÅNulsing, Tanja Lange, Lorenz Panny, Cyprien de Saint
04. Guilhem, and Nigel P. Smart. Post-quantum cryptography - current state and quantum mitigation, 2022.
05. Post-Quantum Cryptography: Current state and quantum mitigation
06. My slides: https://github.com/hamerlinski/slides-btaqc

Contact and Q&A

Contact and Q&A

Blockchain Technology And Quantum Computation

Please contact me using jakub.hamerlinski@cs.put.poznan.pl

Tasks

Tasks

Blockchain Technology And Quantum Computation

01. Create GitHub account (if you don’t have it yet) and repository.
02. Fill form.

Tasks

Blockchain Technology And Quantum Computation

1.1 Create GitHub account using following guide: Create a GitHub account to use with Visual Studio
1.2 Create **public** repository `put-blockchain-implementation` (one per team)

Tasks

Blockchain Technology And Quantum Computation

01. Fill form: https://tinyurl.com/y56zsary

Before next classes

Before next classes

Blockchain Technology And Quantum Computation

Prepare for next lesson by watching `But how does bitcoin actually work?` by 3Blue1Brown at https://www.youtube.com/watch?v=bBC-nXj3Ng4

Questions?

Thank you

Feel free to reach me via LinkedIn

Fin