Skoltech

Course Syllabus

Course Title	Introduction to Blockchain
Course Title (in Russian)	Введение в технологию блокчейн
Lead Instructor	Yanovich, Yury
Co-Instructor	Frolov, Alexey

1. Annotation

Course Description

This course provide an overview of modern blockchain technology and its' practical applications (Cryptocurrency, Certification, Anchoring. Industrial examples.) We will start from basic cryptography and distributed data base systems and show how these tools are used in blockchain. The covered topics are the following:

-) Introduction to cryptography, type of ciphers. Private and Public crypto systems
-) Hash functions.Digital signatures and certificates. Public key infrastructure
-) Secret sharing, esoteric protocols, mental poker
-) Introduction to data base systems. Distributed data base systems
-) Main concept of blockchain. Consensus and Impossibility of Distributed consensus with One Faulty Process
-) Network and computational assumptions. Consensus properties
-) Atomic broadcast. Tendermint. Exonum
-) Cryptocurrency, Certification, Anchoring. Industrial examples

Course Description (in Russian)

Блокчейн (распределенный реестр), предложеный в 2008 как технология в основе криптовалюты Биткоин, нашёл применение во многих областях: государственные реестры, цепочки поставок, финансовый сектор, и другие. Блокчейн основан на красивых математических подходах из криптографии, структур данных и распределенных алгоритмах, таких как криптография с открытым ключом, Меркл деревья и протоколы консенсуса, а также ставит новые вызовы исследователям. В курсе будет рассказано, что такое распределенный реестр, какие теоретические принципы лежат в его основе, а также, какие тренды наблюдаются. Освоение материала требует лишь стандарных знаний студента направления компьютерных наук, а именно:
-) быть знакомым по крайне мере с одним высокоуровневым языком программирования и не бояться сталкиваться с новыми;
-) не пугаться возведения в степень над заданным полем ни на бумаге, ни на компьютере;
-) рисовать графики и выводить текст в Jupyter ноутбуках;
-) понимать, что такое алгоритм.

2. Basic Information

Number of ECTS credits 3

Course Prerequisites / Recommendations

Basic Algorithms, Basic programming, Basic algebra

Type of Assessment Graded

Mapping from grades to percentage:

A: 86

B: 76

C: 66

D: 56

E: 46

F: 0

Term Term 3

Students of Which Programs do You Recommend to Consider this Course as an Elective?

Masters Programs	PhD Programs
Data Science Internet of Things and Wireless Technologies	Computational and Data Science and Engineering

Maximum Number of Students

	Maximum Number of Students
Overall:	60
Per Group (for seminars and labs):	4

Course Stream Science, Technology and Engineering (STE)

3. Course Content

Topic	Summary of Topic	Lectures (# of hours)	Seminars (# of hours)	Labs (# of hours)
Basic introduction into blockchain	Overview of blockchain technology, types of blockchains and industrial examples	1	3	1

Topic	Summary of Topic	Lectures (# of hours)	Seminars (# of hours)	Labs (# of hours)
Introduction into data base systems	Different types of data base systems, queries, transactions, distributed data base systems, security in them	1	3	2
Introduction to cryptography	Type of ciphers. Public and private crypto systems. Hash function. Digital signatures and certificates. Public key infrastructure. Secret sharing, esoteric protocols, mental poker	2	6	2
Practical overview of blockchain technologies	Consensus and Impossibility of Distributed Consensus with One Faulty Process (theorem). Network and computational assumptions (theorem). Consensus properties and examples. Atomic broadcast. Tendermint. Exonum. Cryptocurrency, Certification, Anchoring. Industrial examples	2	6	2

4. Learning Outcomes

Skoltech Learning Outcomes are indicated as per Skoltech Learning Outcomes Framework.

5. Assignments and Grading

Assignment Type	Assignment Summary	% of Final Course Grade
Homework Assignments	Three assignments focusing on blockchain-based programming and cryptography, all executed using Python. The assignments will be based on the class seminars, emphasizing practical application and hands-on experience. The two blockchain assignments delve into programming within blockchain frameworks, showcasing the ability to implement solutions in a decentralized context. Simultaneously, the cryptography assignment hones their skills in leveraging Python to tackle cryptographic challenges.	30
Final Exam	A Set of four problems sourced from a predefined set of questions will be presented, and the task is to address and solve these problems. Their performance will be evaluated based on the quality and accuracy of their solutions.	35

Assignment Type	Assignment Summary	% of Final Course Grade
Final Project	The project assignment allows students to choose a topic from either cryptography or blockchain implementation. For instance, a cryptography-focused project involves implementing a deterministic AKS primality test alongside randomized Miller–Rabin and Fermat tests. The objective is to generate large prime numbers and compare the execution times of these algorithms. On the other hand, a blockchain-focused project centers around creating a document registration system on a decentralized platform. This involves deploying the system on any testnet and interacting with it through Python or JS libraries such as Web3py or Web3js. Students can select a business case, like marriage certificates or agreements, and explore functionalities like checking document validity and genuineness and implementing features like expiration dates. Students are encouraged to showcase problem-solving within the decentralized environment using their chosen project during the presentation.	35

6. Assessment Criteria

Assignment 1 Type

Homework Assignments

Sample of Assignment 1

Find serializable histories in the set of transactions, generate a secret session key for Alice and Bob in Diffie-Hellman protocol, find the secret shared by Blakley's scheme

Develop and investigate the implementation of the Proof-of-Work function that takes the current block header and block calculation difficulty as inputs and returns nonce for this block and the header of a mined block.

Assessment Criteria for Assignment 1

Students receive points based on the results of homework.
The maximum number of points is 100.
Each task gives an equal contribution to the final evaluation. Points for each
the task is depending on its' completeness.
Problem not met - 0 points.
The task is fully completed - the maximum number of points corresponding to it.

Assignment 2 Type Final Project

Sample of Assignment 2

Choose one topic from either cryptography or blockchain implementation.
Example:
1. Prime numbers play an important role in cryptography. Unfortunately, there are still no algorithms for generating arbitrary large prime numbers so typically we generate a big random number and check if it is prime or not. In this project, we will ask you to implement a deterministic AKS primality test as well as randomized Miller–Rabin and Fermat tests. Also, we ask you to compare their execution time.

2. The idea of this project is to create a document registration on a decentralized platform, document can be as simple as a marriage certificates, or simple agreements, etc. Deploy it on any test net and interact with it through python or JS libraries (Web3py or Web3js). You can deploy on your local system, where you can interact with it and check the state of the certificate, i.e. if it is genuine, valid, or fake? additionally, you can put a date in its validity (something like an expiration date). It is completely up to you for what business case you wish to do it. During the presentation, take any problem and show how you resolved it in the decentralized environment using this project.

Students make project in group of 2 or 3. Each student in the same group receive the same point for project.
Student receive points based on the results of project.
The maximum number of points is 100 and student received it for fully completed and well presented project. If project is not fully completed or have some weak points student receive points based on completeness and overall quality of the project. If project isn't started student receive 0 for it.

Assignment 3 Type Final Exam

Sample of Assignment 3

Four problems are given to you:
1. Problem based on cryptography (Theory)
2. Cryptography mathematical solving problem.
3. Blockchain theoretical problem based on concepts
4. Use case scenario and implementation using blockchain (a paragraph).

Assessment Criteria for Assignment 3

The maximum number for each question is 1.
Each task gives an equal contribution to the final evaluation. Points for each the task is depending on its' completeness.
Problem not met - 0 points.
The task is fully completed - the maximum number of points corresponding to it.

7. Textbooks and Internet Resources

You can request at most two required textbooks. Additionaly, you can suggest up to nine recommended textbooks.

Required Textbooks	ISBN-13 (or ISBN-10)
Lipton, Alexander, and Adrien Treccani. Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics. World Scientific, 2021.	9789811221538
B. Schneier Practical cryptography Wiley 2003	0471223573

Recommended Textbooks	ISBN-13 (or ISBN-10)
M.Swan Blockchain: Blueprint for a New Economy. O'REILLY 2015	978-1-491-92049-7

Papers	DOI or URL
Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. – Manubot, 2019.	https://columbia.github.io/ds2-class/papers/nakamoto-bitcoin.pdf
Buterin V. et al. Ethereum white paper: a next generation smart contract & decentralized application platform //First version. – 2014.	https://www.semanticscholar.org/paper/A-Next-Generation-Smart-Contract-and-Decentralized-Buterin/0dbb8a54ca5066b82fa086bbf5db4c54b947719a

Web-resources (links)	Description
https://en.bitcoin.it/wiki/Main_Page	Bitcoin wiki
https://docs.ethhub.io/ethereum-basics/resources/	Has a ton of useful information
https://cryptozombies.io/	Interactive lessons for DApps

8. Facilities

Software
iPython
Visual Studio Code
Jupyter Notebook

Equipment
Personal Computers

9. Additional Notes