FLORIDA ATLANTIC UNIVERSITY

NEW COURSE PROPOSAL
Undergraduate Programs

Department Mathematical Sciences

College Science

*(To obtain a course number, contact **erudolph@fau.edu**)*

UUPC Approval 10/9/2023
UFS Approval
SCNS Submittal
Confirmed
Banner Posted
Catalog

Prefix MAD **Number** 4476	*(L = Lab Course; C = Combined Lecture/Lab; add if appropriate)* **Lab Code**	**Type of Course** Lecture	**Course Title** Cryptography of Blockchain

Credits *(See Definition of a Credit Hour)*: 3

Effective Date *(TERM & YEAR)*: Spring 2024

Grading *(Select One Option)*: Regular (●) Sat/UnSat ( )

Course Description *(Syllabus must be attached, see Template and Guidelines)*

This course provides mathematical foundations of blockchain. Topics include history of blockchain, consensus mechanisms, Hash function, digital signature schemes, zero-knowledge proofs and SNARKs, verifiable random functions, and quantum-safe blockchain.

Prerequisites, with minimum grade* MAD 2104 - Discrete Math and COP 2220 Programming, with a grade of "C" or better.

Corequisites

Registration Controls *(Major, College, Level)*

***Default minimum passing grade is D-.** **Prereqs., Coreqs. & Reg. Controls are enforced for all sections of course**

WAC/Gordon Rule Course

☐ Yes ☑ No

WAC/Gordon Rule criteria must be indicated in syllabus and approval attached to proposal. See WAC Guidelines.

Intellectual Foundations Program (General Education) Requirement *(Select One Option)*

None

General Education criteria must be indicated in the syllabus and approval attached to the proposal. See Intellectual Foundations Guidelines.

Minimum qualifications to teach course

Phd in Mathematics or related fields.

Faculty Contact/Email/Phone

Veronika Kuchta/561-297-3671/vkuchta@fau.edu

List/Attach comments from departments affected by new course

Request for comments sent to Dept EECS on 9/20/2023

Approved by	***Date***
Department Chair	09/19/2023
College Curriculum Chair	9/26/23
College Dean	9/26/23
UUPC Chair Korey Sorge	10/9/2023
Undergraduate Studies Dean Dan Meeroff	10/9/2023
UFS President	
Provost	

Email this form and syllabus to mjenning@fau.edu seven business days before the UUPC meeting.

MAD 4476

Cryptography of Blockchain

Tu 10:00 – 11:20, Th 10:00-11:20

3 credits

Spring, 2024

Prof. Veronika Kuchta

Office: SE43-200

Office hours: WF 11-12

TA name	Veronika Kuchta
Office	SE43- room 200
Office hours	MWF xx:xx – xx:xx
Telephone	561-297-xxxx
Email	vkuchta@fau.edu

Course Description

This course provides mathematical foundations of blockchain. Topics include history of blockchain, consensus mechanisms, Hash function, digital signature schemes, zero-knowledge proofs and SNARKs, verifiable random functions, and quantum-safe blockchain.

A tentative lecture plan includes the following topics:

- History of Blockchain
- Consensus Mechanisms (PBFT, Proof-of-Work, Proof-of-Stake)
- Hash Functions
- (Exotic) Digital Signature Schemes (including blind, threshold, adaptor, multi-/aggregate, ring signatures),
- Zero-Knowledge Proofs and SNARKs,
- Verifiable Random Functions,
- Quantum-safe Blockchain.

Instructional Method: In-Person

Type of Course: Lecture

WAC/Gordon Rule Course: No

IFP course: No

Prerequisites/Corequisites

MAD 2104 - Discrete Math and COP 2220 Programming, with a grade of “C” or better.

Course Objectives/Student Learning Outcomes

This course will introduce the most important and fundamental cryptographic primitives and probability tools which are useful in constructing efficient consensus protocols of Blockchain. After completing the course, students will understand various mathematical foundations of blockchain and will learn how to construct consensus protocols and prove them secure.

Required Texts/Readings

We will provide external reading sources on Canvas before each class. These readings will often serve to expand the acquired knowledge from the class. They are meant to serve as a replacement for the lectures. It is not necessary to read them before coming to the lecture, but pre-reading can help in following the lectures.

Supplementary/Recommended Readings

We will also use some chapters of the book “Foundations of Distributed Consensus and Blockchains” by Elaine Shi. A preliminary draft of the book is freely available online: https://www.distributedconsensus.net/

Course Evaluation Method

The grade for the course will be determined by the following scheme:

Two assignments (40%), Mid-Term Exam (20%), Project (30%).

Assignments: There will be two assignments for the course, each of which counts for 20% of the grade. Assignments should be clearly handwritten or printed on paper or sent by email in PDF format. Late assignments will not be accepted and graded with 0 points.

Mid-Term Exam: Mid-Term exam counts for 20% of the final grade.

Project: A research project will be given for each student, which counts for 30% of the final grade. The purpose is to develop students’ understanding of the current state-of-the-art of the research in blockchain. In the beginning of the semester, a list of research papers will be given. Each student must choose one item in the list and study the paper. Additional research papers (other than from the list) may be acceptable after discussion with the instructor, but each paper must be relevant to the course content. The evaluation of the project consists of two components:

- A report (e.g. 5-8 pages) summarizing the main techniques of the research paper. The report counts for 10% of the total grade.
- An oral exam (45 minutes). The examiners will ask questions on your report; on your understanding of the technical contents of the research paper; and also relevant materials that cover the topics taught during the semester. The oral exam counts for 20% of the total grade.
  The time of the oral exam will be during the exam week. The report should be submitted prior to the oral exam.

Grading scale

At the end of the semester, the following scale for FAU grade will be used.

Total Points	87-100	83-86	77-82	73-76	70-72	67-69	63-66	60-62	57-59	53-56	50-52	<50
Grade	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Course Topical Outline

Week 1: History of Blockchain, Digital Timestamping and Bitcoin paper

Consensus mechanism

Week 2: PBFT, Dolev-Strong Protocol

Week 3: Proof-of-Work (PoW) (Bitcoin paper), Proof-of-Stake (PoS)

Cryptographic primitives in Blockchain

Week 4: Merkle tree, hash functions, digital signature schemes

Week 5: Consensus efficiency: Threshold signatures

Week 6: Account management: Multi- & aggregate signatures

Week 7: Empowering scriptless Blockchain: Adaptor signature

Cryptographic primitives for privacy in Blockchain

Week 8: Blind Signatures

Week 9: Ring Signatures and Confidential Transactions

Week 10: Zero-Knowledge Proofs ZK-SNARKs (with appl. to ZCash)

Week 11 Linear PCPs and pre-processing ZK-SNARKs (Plonk)

Week 12: (post-quantum) ZK-STARKs

Week 13: Scaling the blockchain: ZK-Rollup, recursive ZK-SNARKs

Additional cryptographic primitives in Blockchain:

Week 14: Leader election in consensus: Verifiable Random Functions in Blockchain

Week 15: Randomness in leader election: Verifiable Delay Functions

Make-up Policies on Exams/Tests

If you miss a quiz, you must provide a written, verifiable excuse, if possible, in advance of the scheduled exam. Doctor notes, letters, emails from immediate family members are not accepted as proof of absence from any quizzes. Approval for a make-up quiz must be obtained from your instructor.

Special Course Requirements

Students are expected to be familiar and comply with the standard university policies. In addition, the following policies on assignments should be confirmed.

Collaboration policy on assignments. Collaboration on the assignments is permitted for this course. If you do collaborate, your write-ups must be done independently, and you must acknowledge your collaborators in your write-up. Failure to do so constitutes plagiarism.

Policy on the Recording of Lectures

Because of a new Florida Statute in 2021, the following model language is suggested for inclusion in course syllabi, at the discretion of individual faculty:
Students enrolled in this course may record video or audio of class lectures for their own personal educational use. A class lecture is defined as a formal or methodical oral presentation as part of a university course intended to present information or teach students about a particular subject. Recording class activities other than class lectures, including but not limited to student presentations (whether individually or as part of a group), class discussion (except when incidental to and incorporated within a class lecture), labs, clinical presentations such as patient history, academic exercises involving student participation, test or examination administrations, field trips, and private conversations between students in the class or between a student and the lecturer, is prohibited. Recordings may not be used as a substitute for class participation

or class attendance and may not be published or shared without the written consent of the faculty member. Failure to adhere to these requirements may constitute a violation of the University's Student Code of Conduct and/or the Code of Academic Integrity.

Attendance Policy

Students are expected to attend all of their scheduled University classes and to satisfy all academic objectives as outlined by the instructor. The effect of absences upon grades is determined by the instructor, and the University reserves the right to deal at any time with individual cases of non-attendance. Students are responsible for arranging to make up work missed because of legitimate class absence, such as illness, family emergencies, military obligation, court-imposed legal obligations or participation in University-approved activities. Examples of University-approved reasons for absences include participating on an athletic or scholastic team, musical and theatrical performances and debate activities. It is the student's responsibility to give the instructor notice prior to any anticipated absences and within a reasonable amount of time after an unanticipated absence, ordinarily by the next scheduled class meeting. Instructors must allow each student who is absent for a University-approved reason the opportunity to make up work missed without any reduction in the student's final course grade as a direct result of such absence.

Counseling and Psychological Services (CAPS) Center

Life as a university student can be challenging physically, mentally and emotionally. Students who find stress negatively affecting their ability to achieve academic or personal goals may wish to consider utilizing FAU's Counseling and Psychological Services (CAPS) Center. CAPS provides FAU students a range of services – individual counseling, support meetings, and psychiatric services, to name a few – offered to help improve and maintain emotional well-being. For more information, go to http://www.fau.edu/counseling/

Disability Policy

In compliance with the Americans with Disabilities Act Amendments Act (ADAAA), students who require reasonable accommodations due to a disability to properly execute coursework must register with Student Accessibility Services (SAS) and follow all SAS procedures. SAS has offices across three of FAU's campuses – Boca Raton, Davie and Jupiter – however disability services are available for students on all campuses. For more information, please visit the SAS website at www.fau.edu/sas/.

Code of Academic Integrity

Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see University Regulation 4.001.

If your college has particular policies relating to cheating and plagiarism, state so here or provide a link to the full policy—but be sure the college policy does not conflict with the University Regulation.