CS5298: BLOCKCHAIN AND WEB3.0 SECURITY

Effective Term
Semester A 2026/27

Part I Course Overview

Course Title
Blockchain and Web3.0 Security

Subject Code
CS - Computer Science
Course Number
5298

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
(CS2310 Computer Programming or equivalent)
AND (CS3103 Operating Systems or equivalent)
AND (CS3201 Computer Networks or equivalent)

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course focuses on blockchain technologies and Web3.0 security. We start with the fundamentals of cryptographic primitives that underpin modern blockchain platforms, including collision-resistant hash functions, digital signatures and merkle trees. In the next part, we focus on modern Layer 1 blockchain infrastructures such as Bitcoin, Ethereum, Sui/Aptos, diving deep into the design principles and vulnerabilities behind them (e.g., consensus, smart contracts, EVM). In the last part of our class, we introduce novel Decentralized Finance (DeFi) applications enabled by blockchain technology, including but not limited to automated market makers, decentralized lending, and stablecoins.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understanding and mastering blockchain related concepts and techniques in different domains such as cryptography and consensus.	40	x	x	
2	Analysing the design of existing permissioned and permissionless blockchain systems.	35	x	x	
3	Developing and implementing blockchain system prototypes as well as blockchain-based applications.	25	x	x	

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	The fundamentals of cryptography and distributed systems that underpin modern blockchain platforms will be discussed. Principles, techniques and technologies used in today's permissionless blockchains as well as permissioned blockchains will be discussed. Novel applications enabled by blockchain infrastructure will be also introduced, including smart contracts and decentralized finance.	1, 2, 3	2 hours / week

2	Tutorials	Tutorials will be conducted in laboratory in the forms of discussion, demonstration, and hands-on sessions. Students will work with selected blockchains and ecosystem tools. This provides students with hands-on experience in analyzing the vulnerabilities and complexity of blockchain infrastructures and applications. Students will also develop blockchain prototypes as well as tools to analyze and interact with them in Rust. Students will also get hands-on experience in writing smart contracts in Solidity.	1, 2, 3	1 hour /week

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Mid-term Test	1, 2	10	-	No
2	Project 1	2, 3	10	-	Yes
3	Project 2	1, 2, 3	30	-	Yes

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum marks of the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Mid-term Test

Criterion

Ability to analyze the design principles behind major blockchain infrastructures.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
Project 1

Criterion
Ability to implement basic components of consensus protocols and basic smart contracts in Solidity.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
Project 2

Criterion
Ability to design and implement a complete decentralized application (DApp) on a modern blockchain infrastructure.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)

Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
Examination

Criterion
The exam will include questions to assess the student's ability to explain the principles, techniques and technologies used in blockchains.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Part III Other Information

Keyword Syllabus
The syllabus evolves over time as security topics change. The following is a list of potential course topics:
(1) Cryptographic Primitives: Private Key/Public Key, Cryptographic Hash, Merkle Tree
(2) Consensus in Untrustworthy Environments: PBFT, HotStuff, Zyzzyva
(3) Permissionless Blockchains: Proof of Work (Bitcoin), Proof of Work Challenges, Proof of Stake (Ethereum), New Layer-1 Blockchains (Sui, Aptos)
(5) Smart Contracts: Ethereum Smart Contracts, Solidity, Ethereum Virtual Machine
(6) Exchanges: Cryptocurrency Exchanges, DEXs, Automated Market Algorithms
(7) DeFi: Decentralized Lending, Stablecoins, Maximal Extractable Values

Reading List

Compulsory Readings

	Title
1	-

Additional Readings

	Title
1	An Introduction to Mathematical Cryptography (Jeffrey Hoffstein, Jill Pipher, and J. H. Silverman)
2	Blockchain-Enabled Large-Scale Transaction Management (Mohammad Javad Amiri, Divyakant Agrawal, Amr El Abbadi)