UNSW Course Outline

COMP6451 Cryptocurrency and Distributed Ledger Technologies - 2024

Published on the 14 Feb 2024

General Course Information

Course Code : COMP6451
Year : 2024
Term : Term 1
Teaching Period : T1
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : Multimodal
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Cryptocurrency and Distributed Ledger Technologies are a currently emerging area of technology

that draws on multiple areas of computer science to implement systems that provide secure infrastructure for important societal functions, including financial transactions and the management of commercial trust relationships.

This course aims to develop an understanding of the requirements for electronic payment systems and how these requirements are realised using distributed ledger technologies. The technical ideas to be understood include the key cryptographic constructs, economic incentive mechanisms and distributed algorithms underpinning cryptocurrencies such as Bitcoin and Ethereum. The concept of smart contract will be introduced, and the course aims to develop a basic facility with programming smart contracts on one cryptocurrency platform. The course also aims to introduce students to the broader context of the range of alternate designs for distributed ledger technologies, the range of potential applications for these technologies, and the socio-economic, ethical and legal dimensions of their use.

Course Aims

The aim of the course is to provide an overview of this area and to introduce students to the underpinning technical areas of computer science including cryptography, distributed computing, and secure coding. The course provides an initial exposure to the novel concerns in application programming that these technologies introduce. Due to the socio-technical nature of the field, the course also aims to develop students' knowledge of the applications being addressed using the technology, and the ethical, economic and legal issues that are inherent in these applications.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Understand the concept of decentralisation and the functional and security requirements for cryptocurrency and distributed ledger applications
CLO2 : Understand the functioning of the proof of work protocol, cryptographic mechanisms and transactional structures underpinning the design of cryptocurrencies including Bitcoin and Ethereum
CLO3 : Be able to program and deploy simple smart contracts on the Ethereum platform
CLO4 : Be aware of the range of design dimensions of distributed ledger technologies, including in consensus protocol design, open versus closed blockchains, levels of privacy, transactional expressiveness, and governance structure
CLO5 : Have an awareness of key aspects of the ethical, socio-economic and legal dimensions of cryptocurrency and distributed ledger technologies, including their positive and negative repercussions and challenges for regulatory authorities

Course Learning Outcomes	Assessment Item
CLO1 : Understand the concept of decentralisation and the functional and security requirements for cryptocurrency and distributed ledger applications	• Written Assignment
CLO2 : Understand the functioning of the proof of work protocol, cryptographic mechanisms and transactional structures underpinning the design of cryptocurrencies including Bitcoin and Ethereum	• Written Assignment
CLO3 : Be able to program and deploy simple smart contracts on the Ethereum platform	• Programming Assignment
CLO4 : Be aware of the range of design dimensions of distributed ledger technologies, including in consensus protocol design, open versus closed blockchains, levels of privacy, transactional expressiveness, and governance structure	• Research Project
CLO5 : Have an awareness of key aspects of the ethical, socio-economic and legal dimensions of cryptocurrency and distributed ledger technologies, including their positive and negative repercussions and challenges for regulatory authorities	• Research Project

Learning and Teaching Technologies

Moodle - Learning Management System

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Written Assignment Assessment Format: Individual	30%	Due Date: March 8th
Programming Assignment Assessment Format: Individual	35%	Due Date: March 28th
Research Project Assessment Format: Individual	35%	Due Date: April 19th

Assessment Details

Written Assignment

Assessment Overview

A written assignment comprised of 5-6 questions concerning fundamental cryptographic background, protocols and economic design aspects of cryptocurrency systems. Answering these questions may require mathematical analysis using discrete mathematics concepts. Answer length may be up to one page per question.

The submission will be marked against assessment criteria. Feedback will be provided online.

Course Learning Outcomes

- CLO1 : Understand the concept of decentralisation and the functional and security requirements for cryptocurrency and distributed ledger applications
- CLO2 : Understand the functioning of the proof of work protocol, cryptographic mechanisms and transactional structures underpinning the design of cryptocurrencies including Bitcoin and Ethereum

Programming Assignment

Assessment Overview

A programming assignment concerned with the development of a smart contract in the Solidity programming language on the Ethereum platform. In addition to the code, deliverables include evidence of testing and a written report. The report should explain the design rationale for the code developed, map requirements to code components, analyse non-functional aspects of the design (security and performance), and explain the test methodology.

The submission will be marked against assessment criteria. Feedback will be provided online.

Course Learning Outcomes

- CLO3 : Be able to program and deploy simple smart contracts on the Ethereum platform

Research Project

Assessment Overview

An essay of up to 5,000 words based on individual research into an advanced technical topic in current cryptocurrency research and development, selected from a list of options provided in the assignment specification. The essay will be expected to explain a problem area, provide an up to date historical overview of work towards its solution, describe two solution approaches in greater detail, and provide a comparative analysis of these two solutions.

The submission will be marked against assessment criteria. Feedback will be provided online.

Course Learning Outcomes

- CLO4 : Be aware of the range of design dimensions of distributed ledger technologies, including in consensus protocol design, open versus closed blockchains, levels of privacy, transactional expressiveness, and governance structure
- CLO5 : Have an awareness of key aspects of the ethical, socio-economic and legal dimensions of cryptocurrency and distributed ledger technologies, including their positive and negative repercussions and challenges for regulatory authorities

General Assessment Information

Grading Basis

Standard

Course Schedule

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

Syllabus

- Cryptographic background: encryption, signatures, hash functions
- Early payment systems, cryptocurrency designs, and Bitcoin precursors
- Bitcoin protocol and network
- Bitcoin transaction structure, Bitcoin script
- Wallets and exchanges
- Ethereum protocol, blockchain and virtual machine
- Smart contracts and Solidity programming
- Cryptocurrency mining
- Alternatives to Proof of Work
- Consortium/permissioned chains and stablecoins
- Privacy in blockchains
- Legal considerations

Course Resources

Prescribed Resources

Prequisites: COMP2521 or COMP9024

Recommended Resources

The required textbook for this course is *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* Andrew Miller, Arvind Narayanan, Edward Felten, Joseph Bonneau, and Steven Goldfeder. Princeton University Press 2016.

Additional notes are made available on the course Moodle page.

Course Evaluation and Development

The course previously ran in Summer 2018-19 with a small group of students. Iterations for

larger classes in 2021-2023, were taught online, leading to the development of pre-recorded lectures. These will be improved and extended in the current iteration, based on feedback from 2021-2023 students. The field is in an early state of development and highly dynamic, so revisions to this course may be frequent.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Ron Van der Meyden					Yes	Yes

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism
- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. *Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient

time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the course convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum queries, cannot understand the lecturer)