COMP6451 Cryptocurrency and Distributed Ledger Technologies Course Information for Session 1 2021

(The present document is available online at http://www.cse.unsw.edu.au/~cs6451).

Staff

Name	Role	location	phone	email
Ron van der Meyden	lecturer-in-charge	Office 217F, CSE (K17)	9385 6922	R.VanderMeyden@unsw.edu.au

Class Times

Lectures are online via the Course Moodle page. Live discusion sessions will be held in one of the following time slots. See Moodle for details.

Tue 2:00pm - 4:00pm
Thus 3:00pm - 5:00pm

Lectures will run weeks 1-5 and 7-10.

This course has no tutorials

Course Objectives

The 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 Overview by Keywords

Cryptocurrency, Blockchain, Distributed Ledger Technology, Bitcoin, Ethereum, Smart Contracts, Cryptography, Distributed Systems

Lectures and Readings

Lectures and readings for the course will be posted on the class Moodle page.

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

The course uses lectures and individual work to develop an understanding of the requirements for electronic payment systems and the realisation of these requirements using distributed ledger technologies. A programming exercise on the Ethereum platform is used to give hands on experience with a particular cryptocurrency platform and the concept of smart contracts. The intended student body for the course is computer science students and the focus of the course is primarily technical, but it includes components relating to the ethical, socio-economic and legal context for these technologies. The broader scope for application of these technologies is addressed via lectures and an individual research assignment that will give students scope to explore applications of personal interest.

Learning Outcomes

- Understand the concept of decentralisation and the functional and security requirements for cryptocurrency and distributed ledger applications.
- Understand the functioning of the proof of work protocol, cryptographic mechanisms and transactional structures underpinning the design of cryptocurrencies including Bitcoin and Ethereum.
- Be able to program and deploy simple smart contracts on the Ethereum platform
- 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.

- 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.

Graduate Attributes

This course address the following elements of the UNSW graduate attributes:

- **understanding of their discipline in its interdisciplinary context** :
  The topic of this course is inherently interdisciplinary. Cryptocurrency systems involve technical ideas from cryptography (based in mathematics), distributed computing, and economic game theory. Cryptocurrency and other blockchain applications are socio-technical systems, involving issues such as monetary theory and financial regulation, privacy, and contract law. The focus of the course is technical, but lectures will cover some of these interdisciplinary connections.
- **rigorous in their analysis, critique and reflection**:
  Technical components of the course will require rigour in dealing with the mathematical foundations of cryptography. The individual research project will give students an opportunity to develop their analytic and critical skills.
- **able to apply their knowledge and skills to solving problems**:
  The programming and written homework will require problem solving.
- **capable of effective communication**:
  The individual research project will exercise your communication skills.

Prerequisites and Follow-Ons

Prequisites: COMP2521 or COMP9024

Text Book

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.

Consultations

Time will be allocated during lectures for ad hoc questions concerning the course contents. (Any difficulties that you have in understanding the content are likely to be shared by other students, who may also benefit from the answers given.)

The lecturer will be available immediately after lectures for consultation, but may schedule an appointment for issues requiring extended discussion. You may also schedule an appointment by email request.

Assessment Summary

The final mark is determined as the sum of the marks for the assessable components of the course:

- 30% Written assignment
- 35% Individual programming assignment
- 35% Individual research project

You can inspect the current state of your mark record by using Moodle.

All marks must be finalised by the end of stuvac. If you think there is a problem with any of your marks then you need to advise us by emailing us within two weeks of the mark being released, and, in all cases before the end of stuvac. No marks will be changed after the end of stuvac.

Late Penalties

Late homework submissions will be penalised by deducting 10% of the maximum homework grade per day late. If you have any valid grounds for failure to submit homework, you should submit an official request for special consideration.

Plagiarism, special considerations, supplementary exams

You are responsible for being familiar with the CSE policies concerning special consideration and supplementary examinations . Be sure to note the dates for final exams and CSE supplementary exams advertised early in the session. You are responsible for being available on the examination dates and on the CSE supplementary exam date in the case you are granted a supplementary exam. Requests for exams on an alternate date on the grounds that you are not available to take the exam due to travel WILL be rejected. Students are therefore very strongly advised not to book travel that conflicts with any potential exam dates, including the supplementary exam date.

Unless clearly indicated otherwise (see below) submitted work is expected to be your individual effort. Recall that you are bound by the UNSW Plagiarism Policy.

You are allowed in this course to confer with other students to clarify the statement of a problem and discuss general approaches to the solution of related problems, but the solution submitted should be solely the work of the individual.

Keeping Informed and Staying in Touch

Important information concerning this course may be communicated via the following media. Students are responsible for regularly checking these channels for communications.

- **Course Web Site:** Important notices related to this course will be displayed on the *Moodle home page* for this course.
- **Email:** Urgent information may also be sent to your CSE email account. Requests of a confidential nature should be sent to the instructor email accounts noted above, with "COMP6451" in the header. General questions likely to be of interest to other students should be raised in class.

Course Evaluation and Development

The course previously ran in Summer 2018-19 with a small group of students, whose feedback has been taken into account in the present iteration. The present iteration, with a larger number of students, will provide better information for future revisions. The field is in an early state of development and highly dynamic, so revisions to this course may be frequent.