

## CS3BC20-Blockchain Computing

**Module Provider:** Computer Science

**Number of credits:** 10 [5 ECTS credits]

**Level:**6

**Terms in which taught:** Spring term module

**Pre-requisites:** CS2DI17 Databases and Information Security

**Non-modular pre-requisites:**

**Co-requisites:**

**Modules excluded:**

**Current from:** 2020/1

**Module Convenor:** Prof Atta Badii

**Email:** [atta.badii@reading.ac.uk](mailto:atta.badii@reading.ac.uk)

**Type of module:**

### **Summary module description:**

The advent of Blockchain technologies as a confluence of distributed systems for transferring value, asymmetric encryption and consensus seeking algorithms has evolved through a trend from web2.0, web3.0, and crowdsourcing promising computing for decentralisation and democratisation of transaction processing.

The increasing number of potential application domains being considered for the take-up and scale-up of this technology makes a compelling case for the provision of this course. This is to ensure that our Computer Science graduates' awareness of latest technological developments and their employability prospects are enhanced through gaining a sufficiently deep understanding of this emerging technology.

This modules will deliver a theoretical and practical implementation level understanding of the various layers of the Blockchain technology stack including asymmetric encryption, mining (Proof-of-Work), Proof-of-Stake consensus algorithms, Blockchain validation and integration as well as the potential Ethical, Legal and Societal issues arising from failure to incorporate the appropriate security-privacy safeguards.

### **Aims:**

The module provides students with a theoretical and practical understanding of the Blockchain architectural layers involving the implementation of the primary layers, as a simulation of a basic Blockchain, to include transactions processing, blocks structuring, mining and validation. This will include asymmetric encryption, mining (Proof-of-Work), Proof-of-Stake, consensus algorithms, Blockchain validation and privacy-aware integration.

This module also encourages students to develop a set of professional skills, such as an ethically reflective approach to system design, privacy-preserving design, evolutionary system design, modular design and conformance testing.

### **Assessable learning outcomes:**

At the end of the module studies, students should be able to:

- Conceptualise the distributed ledger architecture at various levels of abstraction
- Understand the theoretical underpinning of Blockchain architectural layers
- Understand the issues relating to the efficient, secure and privacy-aware deployment of Blockchain layers
- Implement the primary layers of a Blockchain as a laboratory simulation of a small-scale Blockchain. This will help the students assimilate the subject more deeply and gain a systemic understanding of the Blockchain architecture through experience in analysing and building the primary Blockchain components and their integration.

**Additional outcomes:**

Building on the Software Engineering, and, System Development Methodology learning acquired in parts 1 & 2; understanding the implications of a design commitment to Responsible Innovation; reflecting on the rationale, benefits and possible societal impacts of deployment of Blockchain for various applications.

**Outline content:**

- Introduction to the fundamental concepts of a distributed trustless ledger such as immutability, irreversibility, the layers of Blockchain technology stack; including overview of the architectural layers of a Blockchain, network (peer-to-peer) and the data structures
- Transactions processing, hashing, asymmetric encryption
- Digital signature, consensus algorithms
- Consensus reaching using variants of Proof-of-Work and Proof-of-Stake algorithms
- Smart contracts
- Concepts re integrity and resolution of Blockchain, avoiding duplication of work
- Byzantine Fault Tolerance: fault tolerance amongst the peer-to-peer network of nodes
- Merkle root algorithm, forks resolution, interoperability
- Security & privacy, public versus private (Permissioned, Permissionless) Blockchain
- Ethically and socially responsible design of Blockchains

**Global context:**

The content of this module will be consistent with the latest implementations of Blockchain as per standard industry Blockchain platforms e.g. as provided by leading players such as Ethereum.

**Brief description of teaching and learning methods:**

This will include an interleaving of lectures and closely-coupled laboratory-based and tutorially-supported structured exercises enabling the students to incrementally develop deeper understanding of the main elements of a basic Blockchain. The students will then be able to use the resulting implementation to form the basis of further work for the Coursework.

**Contact hours:**

	Autumn	Spring	Summer
Lectures		10	
Practicals classes and workshops		10	
<b>Guided independent study:</b>			

Wider reading (independent)		16	
Wider reading (directed)		10	
Exam revision/preparation		25	
Peer assisted learning		3	
Preparation of practical report		6	
Completion of formative assessment tasks		18	
Reflection		2	
Total hours by term	0	100	0
Total hours for module	100		

#### Summative Assessment Methods:

Method	Percentage
Written exam	70
Set exercise	30

#### Summative assessment- Examinations:

One 2-hour examination paper in May/June.

#### Summative assessment- Coursework and in-class tests:

A coursework will be built on the exercises in the laboratory sessions to extend the basic simulation developed to include consensus resolution and validation of Blockchain within a small simulated Blockchain.

#### Formative assessment methods:

Practical exercises are made available with worked examples and students have the opportunity to obtain feedback on their attempts at solving the problems set e.g. through comparing their answers with the structured model answers provided and/or receiving personal feedback on their work through the tutorial sessions.

#### Penalties for late submission:

The Module Convenor will apply the following penalties for work submitted late:

- where the piece of work is submitted after the original deadline (or any formally agreed extension to the deadline): 10% of the total marks available for that piece of work will be deducted from the mark for each working day<sup>[1]</sup> (or part thereof) following the deadline up to a total of five working days;
- where the piece of work is submitted more than five working days after the original deadline (or any formally agreed extension to the deadline): a mark of zero will be recorded.

The University policy statement on penalties for late submission can be found

at: <http://www.reading.ac.uk/web/FILES/qualitysupport/penaltiesforlatesubmission.pdf>

You are strongly advised to ensure that coursework is submitted by the relevant deadline. You should note that it is advisable to submit work in an unfinished state rather than to fail to submit any work.

**Assessment requirements for a pass:**

A mark of 40% overall

**Reassessment arrangements:**

One 2-hour examination paper in August/September. Note that the resit module mark will be the higher of (a) the mark from this resit exam and (b) an average of this resit exam mark and previous coursework marks, weighted as per the first attempt (70% exam, 30% coursework).

**Additional Costs (specified where applicable):**

**Last updated:** 13 August 2020

**THE INFORMATION CONTAINED IN THIS MODULE DESCRIPTION DOES NOT FORM ANY PART OF A STUDENT'S CONTRACT.**