

CST4025

Blockchain Development

Module Leader: Dr Ian Mitchell

Term: 2019-20

Duration of the module: 24 weeks

Document version: 1

Online location of handbook (delete if module handbook is only available online)

This handbook can also be accessed via MyLearning.

Other formats available

This handbook is available in a large print format. If you would like a large print copy or have other requirements for the handbook, please contact the Disability Support Service (disability@mdx.ac.uk, +44 (0)20 8411 4945).

Disclaimer

The material in this handbook is as accurate as possible at the date of production. You will be notified of any minor changes. If there are any major changes to the module you will be consulted prior to the changes being confirmed.

Other documents

Your module handbook should be read and used alongside your programme handbook and the information available to all students on My Learning, including the Academic Regulations. Your programme handbook can be found on the My Learning programme page.

Contents

1	Module Introduction	1
1.1	The Module Team	1
1.2	Staff Student Communication	2
1.3	Module Overview	2
1.3.1	UNISTATS - learning & teaching	3
1.4	Learning Resources	3
1.5	Indicative Lecture Plan.	4
2	Research Ethics	7
3	Assessment	9
4	Coursework 1	11
4.1	Instructions	11
4.2	Introduction	11
4.3	Problem Specification	12
4.4	Data Model	12
4.4.1	Introduction	12
4.4.2	Participants	12
4.4.3	Assets	12
4.4.4	Transactions	13
4.4.5	Comments	13
4.5	Documentation	13
5	Coursework 2	15
5.1	Instructions	15
5.2	Introduction	15

5.3	Data Model	16
5.4	Access Control language	16
5.5	Business Logic	16
5.6	Presentation	16
5.6.1	Comments	17
5.7	Documentation	17
6	Deferred Coursework	19
6.1	Instructions for deferrals before 1st June 2020	19
6.2	Instruction for deferrals after 1st June 2020	19
7	Resit Coursework	21
7.1	Instruction for Resits	21


Chapter 1

Module Introduction

It is necessary for all students of CST4025 to attend 75% of lab sessions. Students with less than 75% attendance will fail the module and be given a grade X. This has serious implications, since the allocation of an X grade does not allow you to resit the module and since CST4025 and require you to retake the module at a later date with a further financial penalty.

Naturally, there are occasions when you may not be able to attend a lab session. Usually these absences are due to unforeseen circumstance and can be quickly remedied by doing extra work to catch-up. Prolonged absence due to exceptional circumstances need to be raised with Dr Ian Mitchell immediately via email and a deferral request submitted as soon as possible to unihelpdesk.

1.1 The Module Team

Dr Ian Mitchell		
	Role:	Module Leader
	Room:	T108
	Email:	i.mitchell@mdx.ac.uk
	Telephone:	0208-411-6014

1.2 Staff Student Communication

Students may contact staff via e-mail, phone, by dropping in to staff office hours, and by making an appointment to see them outside office hours. Staff will contact students by e-mail, phone, the My Learning module page and via lectures and seminars.

The team may send urgent group and/or individual messages about the module to you by email, so it is important that you read your University email regularly. All staff have office hours, it is not necessary to book an appointment during these hours.

In the first instance problems should be dealt with by talking to a member of the module team. You can give feedback on this module to the module leader, your Student Voice Leader, and through the end of module evaluation survey.

1.3 Module Overview

Aims

Blockchain Technology is changing how organisations communicate and operate, with this change there is a challenge and opportunity for Blockchain developers. This module aims to convey the required knowledge underpinning blockchain technology in order to enable students to apply it to develop solutions to practical problems.

Knowledge

On completion of this module, the successful student will be able to:

- Appraise blockchain types and holistically explain blockchain anatomy
- Analyse a domain specific problem and determine the applicability of a blockchain solution to that problem

Skill

This module will call for the successful student to demonstrate:

- The design and development of effective blockchain applications

Syllabus

- Asynchronous and procedural programming pertaining to blockchain applications
- Blockchain data structures for distributed ledger systems

- Access Control Language for distributed ledger systems
- Implementing business logic for a blockchain solution
- Blockchain and complex system development
- Permissioned Blockchain Technologies
- Consensus Engineering
- Blockchain Engineering
- Blockchain Anatomy

1.3.1 UNISTATS - learning & teaching

- 12*1 hour lectures
- 12*2 hour labs

The proposed number of scheduled teaching hours: 36

Placement Activity: N/A

Independent Study: 12*9.5 hours

The proposed number of hours a student should complete independent study: 114

1.4 Learning Resources

The module team are here to help and support you achieve your goals. One of the key elements to successfully completing this module is engaging with all of the learning opportunities we offer as well and working with your peers to support one another.

Participation and engagement

This module is designed as a combination of contact sessions and independent study. This means you must attend all the allocated sessions and you must work on your own outside them. Students are expected to take an active part in all learning sessions; lectures, lab sessions, practical classes, seminars and workshops.

Student attendance is monitored during *labs*, and any unexplained absences will be followed up via e-mail. If for any reason you are unable to attend a session you must inform the module leader.

To make the most of this module please complete the following every week

- Read through the notes making a note of any points you need to discuss with your tutor.

- **Complete the set activities before the next session, making a note of any points you need to discuss with your tutor.**
- **Go to the module My Learning page, make use of extra material, view the podcasts, and access the activity solutions. Make a note of anything you wish to discuss with your tutor.**
- **Complete further reading from the core text online.**

The module team is committed to support you and your fellow students whilst you undertake this module. In order for you to get the most out of sessions you need to come prepared and ready to contribute. Please ensure that any work set by the team has been completed before workshops. After each class please review what has been covered and make a note of anything you would like clarification on.

It is important that you are respectful and supportive to your fellow students and tutors. Adopting this approach will create a positive atmosphere within sessions and is something you can use in your professional life.

To access some of the rooms and specialist space used for this module you will need your University ID card. Please remember that your University ID should be carried with you always.

Lateness policy

Please ensure you are on time to sessions as tutors will start sessions promptly. Please note that if you are more than 15 minutes late you will not be permitted to join the session.

Mobile phones

Please have your phones on silent throughout the session and only use them in an emergency.

1.5 Indicative Lecture Plan.

Week	Title
1	Introduction to Blockchain
2	Composer: Data Modelling
3	Composer: Access Control Language
4	Case Study and Formative Feedback
5	Asynchronous Programming & Promises
6	Composer: Node.js I
7	Composer: Node.js II
8	Consensus Engineering
9	Smart Contracts
10	Case Study and Formative Feedback
11	Case Study and Formative Feedback
12	Presentation

Table 1.1: Lecture Plan, these are indicative titles

Chapter 2

Research Ethics

The teaching, learning, assessment and research activities undertaken in this module have been considered and are not likely to require ethical approval. However, please seek advice if undertaking the module entails carrying out any research activities involving human participants, human data, animals/animal products, precious artefacts, materials or data systems. If you submit work that includes data gathered from or about people, this may be treated as academic misconduct and could lead to fail grade being awarded. Research ethics approval seeks to ensure all research is designed and undertaken according to certain principles of ethical research. These include:

1. Primary concern must be given to the safety, welfare and dignity of participants, researchers, colleagues, the environment and the wider community
2. Consideration of risks should be undertaken before research commences with the aim of minimising risks to those involved i.e. human participants or animal subjects, colleagues, the environment and the wider community, as well as actual or potential risks to those directly or indirectly affected by the research.
3. Informed consent should be freely given by participants, and by a trained person when collecting or analysing human tissue (details on accessing and completing online training for gaining informed consent for HTA purposes can be found below in Section 8).
4. Respect for the privacy, confidentiality and anonymity of participants
5. Consideration of the rights of people who may be vulnerable (by virtue of perceived or actual differences in their social status, ethnic origin, gender, mental capacities, or other such characteristics) who may be less competent or able to refuse to give consent to participate
6. Researchers have a responsibility to the general public and to their profession; as such they should balance the anticipated benefits of their research against potential harm, misuse or abuse which must be avoided
7. Researchers must demonstrate the highest standards of ethical conduct and research integrity. They must work within the limits of their skills, training and experience, and refrain from exploitation, dishonesty, plagiarism, infringement of intellectual property rights and the fabrication of research results. They should

declare any actual or potential conflicts of interest, and where necessary take steps to resolve them.

- 8. When using human tissues for research, Human Tissue Act and Human Tissue Authority (HTA) requirements must be met. Please contact the relevant designated person (DP) in your department or the HTA Designated Individual (DI) (Dr Lucy Ghali - L.Ghali@mdx.ac.uk). Further information is provided below in this section: "Human Tissue Authority Information", see 'Governance Structure' document and SOPs etc.**

- 9. Research should not involve any illegal activity, and researchers must comply with all relevant laws.**

For more information about ethics go to the Middlesex Online Research Ethics (MORE) system which has information and guidance to help you meet the highest standards of ethical research using this link: <https://MOREform.mdx.ac.uk>. Information and further guidance on how to complete a research ethics application form (e.g., video guides and templates) can be found on the MORE MyLearning site¹: <http://mdx.mrooms.net/enrol/index.php?id=12277> (Log in required)

¹Middlesex University Definition of Research document can be located on this site

Chapter 3

Assessment

Formative assessment: Formative assessments do not directly contribute to the overall module mark but they do provide an important opportunity to receive feedback on your learning. They provide an opportunity to evaluate and reflect on your understanding of what you have learnt. They also help your tutors identify what further support and guidance can be given to improve your grade.

On this module you will have the following formal assessment opportunities: learning weeks 4 and 10–11.

Summative assessment: Summative assessment is the assessed work that determines the overall module grade. It is the way the University verifies that students have met the learning outcomes at the appropriate level.

There are *two* assessment components in this module: *Coursework 1* and *Coursework 2*.

Feedback on your assignments

Feedback will normally be provided within 15 working days of the published assessment component submission date.

Overall module grade

Each component of assessment will be marked as a percentage. To produce the overall module grade a weighted average percentage will be calculated and then converted to a 20-point grade using the scale below.

Assessment process

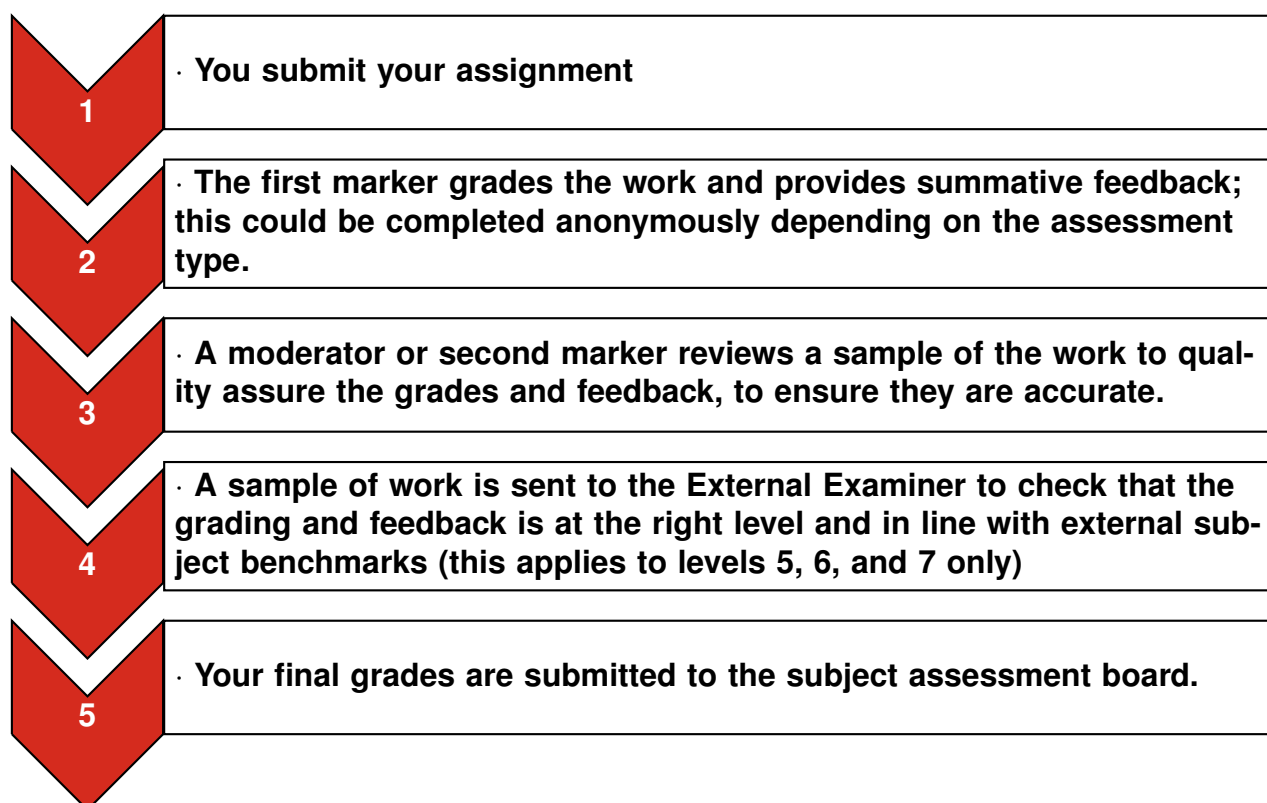
CST4025 is composed of *two* in-course assignments. These deadlines are correct, but may be subject to change. Table 3.1 shows the important dates associated with

each of the in-course assignments. The table also indicates that the assessment weighting, which gives the grand total of 100%. Your final grade for CST4025 will be calculated from adding each of these sub-totals for the in-course assignments, which must exceed 39.5% to pass.

Assessment	Formative Feedback	Deadline	%
Coursework 1	Week 4	3 rd November 2019	25
Coursework 2	Week 10–11	5 th January 2020	75
Deferred Coursework 1	N/A	1 st August 2020	25
Deferred Coursework 2	N/A	1 st August 2020	75
Resit Coursework 1	N/A	1 st August 2020	25
Resit Coursework 2	N/A	1 st August 2020	75

Table 3.1: In-course Assignments for CST4025

The following diagram provides an overview of the marking process for your module assessment. Details of the programme external examiner can be found in the programme handbook.



Chapter 4

Coursework 1

CST4025
Blockchain Development
Coursework 1: Data Modelling
Academic Year: 2019-20
Deadline: 3rd November 2019
Coursework is worth 25% of the module.

4.1 Instructions

The aims of this coursework is to build a data model of a blockchain application. The coursework is to be completed:

- as an individual

4.2 Introduction

You are to develop a blockchain application to a problem specification designed by you. Be aware of choosing trivial problem specifications, since whilst they are easy to develop for solutions for, they do not have the complexity to exhibit the technical requirements to match some of the assessment criteria.

This part of the coursework is for data modelling and will form a the data model for coursework 2. Getting this correct is an important and incremental step.

A suggested plan for this coursework is as follows:

1. Write problem specification and its suitability for a blockchain application
2. Model participants, assets and Transactions
3. Code Participants, Assets and Transactions
4. Get Formative Feedback and comment your code

5. Make any modifications and submit

4.3 Problem Specification

The problem specification should be written in Chapter 1 of the document and contain the following sections:

- 1. Use Case.** Create a subsection in Use Case model
- 2. Description.** An explanation of no more than 250 words explaining the use case model
- 3. Applicability** How applicable is the problem definition to blockchain, use the flowchart in lecture 1 and explain each stage in an itemised list.

4.4 Data Model

The Data Model should be written in Chapter 2 of the document and contain the following sections:

- 1. Introduction**
- 2. Participants**
- 3. Assets**
- 4. Transactions**

4.4.1 Introduction

Include a class diagram of your problem specification. Any assumptions or explanations should be included and not exceed 100 words.

4.4.2 Participants

Based on your class diagram write the CTO code for the participants. Any assumptions or explanations should be included and not exceed 100 words.

4.4.3 Assets

Based on your class diagram write the CTO code for the assets. Any assumptions or explanations should be included and not exceed 100 words.

4.4.4 Transactions

Based on your class diagram write the CTO code for the transactions. Any assumptions or explanations should be included and not exceed 100 words.

4.4.5 Comments

All the above code should include appropriate comments.

4.5 Documentation

All submissions are to be completed in \LaTeX document template available on myLearning.

Assessment.

Assessment Criteria	Mark
§5.2 Introduction <ol style="list-style-type: none"> 1. Originality: 5% 2. Specification & Use Case: 10% 3. Applicability: 5% 	20%
§4.4 Data Model <ol style="list-style-type: none"> 1. Participants: 20% 2. Assets: 20% 3. Transactions: 20% 4. Comments: 10% 	70%
§5.7 Documentation <ol style="list-style-type: none"> 1. Template: 2% 2. References: 5% 3. Structure: 3% 	10%
Total	100%

Chapter 5

Coursework 2

CST4025
Blockchain Development
Coursework 2: Blockchain Application
Academic Year: 2019-20
Deadline: 5th January 2020
Coursework is worth 75% of the module.

5.1 Instructions

The aims of this coursework is to build a blockchain application. The coursework is to be completed:

- as an individual

5.2 Introduction

You are to develop a blockchain application to a problem specification designed by you.

A suggested plan for this coursework is as follows:

1. Write Access Control in ACL
2. Design a sequence diagram
3. Write prototype Node.js code
4. Complete BNA and test
5. Get Formative Feedback and comment your code
6. Make any modifications and submit

5.3 Data Model

Include a CTO listing from coursework 1. This is to provide some continuity between coursework 1 and 2, as well as provide the opportunity to show any improvements. Any improvements from the last submission should be explained and not exceed 250 words.

5.4 Access Control language

Include a complete ACL listing for your blockchain application. Any assumptions or explanations should be included and not exceed 250 words.

5.5 Business Logic

Include a complete sequence diagram for the system, this should show key components of the system and how they interact via transactions.

For each transaction include:

- a subsection for the transaction, e.g., if my transaction is identified as `'trade'` then the associated subsection should be named likewise
- Associated code
- Any assumptions, issues or restrictions that you have encountered. Remember sometimes the functionality can have bugs or issues that you could not resolve. These should not exceed 100 words per transaction subsection.
- Relate your transaction to the sequence diagram

5.6 Presentation

The duration of each presentation should not exceed 5 minutes. Each presentation should show screenshots of the blockchain application developed above of the following:

1. Use Case Diagram and a brief outline of the problem
2. Show blockchain before transactions occur
3. Users: show successful transactions between participants and assets
4. Users: show unsuccessful transaction between participants and assets, this should either be because of the user does not have sufficient access privileges or the business logic prevents this from happening

5. Show blockchain after transactions occur, highlighting where the event has updated the transaction

5.6.1 Comments

All the above code should include appropriate comments.

5.7 Documentation

All submissions are to be completed in \LaTeX document template available on myLearning. /

Assessment.

Assessment Criteria	Mark
§5.3 Introduction	5%
1. Continuity & Improvements: 5%	
§5.4 Access Control	35%
1. Order of ACL: 10%	
2. ACL participant access: 10%	
3. ACL conditions: 10%	
4. Comments: 5%	
§5.3 Business Logic	45%
1. Sequence Diagram: 10%	
2. Unrestricted transactions: 10%	
3. Restricted transactions: 20%	
4. Comments: 5%	

Assessment Criteria	Mark
§5.3 Presentation 1. Prepared Slides: 2% 2. Slide Content: 2% 3. Body Language: 2% 4. Oral Content: 2%	8%
§5.7 Documentation 1. Template: 2% 2. References: 2% 3. Structure: 3%	7%
Total	100%

Chapter 6

Deferred Coursework

6.1 Instructions for deferrals before 1st June 2020

If your deferral has been granted before 1st June 2020, then submit the coursework you deferred by 1st May 2020. If you deferred:

1. Coursework 1, then complete the Data Modelling coursework specification in Chapter 4 and submit via MyLearning by 1st May 2020
2. Coursework 2, then complete the Blockchain Application coursework in Chapter 5 and submit via MyLearning by 1st May 2020

6.2 Instruction for deferrals after 1st June 2020

If your deferral has been granted after June then submit the coursework you deferred by 1st August 2020.

If you deferred:

1. Coursework 1, then complete the Data Modelling coursework specification in Chapter 4 and submit via MyLearning by 1st August 2020
2. Coursework 2, then complete the Blockchain Application coursework in Chapter 5 and submit via MyLearning by 1st August 2020

Chapter 7

Resit Coursework

7.1 Instruction for Resits

If you have a resit coursework code for your first attempt then, resubmit the coursework you failed:

1. If you failed Coursework 1, then complete the Data Modelling coursework specification in Chapter 4 and submit via MyLearning by 1st August 2020
2. If you failed Coursework 2, then complete the Blockchain Application coursework in Chapter 5 and submit via MyLearning by 1st August 2020

Bibliography

- [1] Hyperledger architecture, volume 1, 2017.
- [2] Hyperledger architecture, volume 2, 2018.
- [3] Federal Information Processing Standards (FIPS) 180-1. Secure hash standard. 1996.
- [4] Jean-Paul Bahsoun, Rachid Guerraoui, and Ali Shoker. Making bft protocols really adaptive. In *2015 IEEE International Parallel and Distributed Processing Symposium*, pages 904–913. IEEE, 2015.
- [5] Martijn Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin.
- [6] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.
- [7] David F Ferraiolo, Ravi Sandhu, Serban Gavrila, D Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):224–274, 2001.
- [8] Nitin Gaur, Luc Desrosiers, Petr Novotny, Venkatraman Ramakrishna, Anthony O’Dowd, and Salman A. Baset. *Hands-on Blockchain with Hyperledger: Building Decentralised Applications with Hyperledger Fabric and Composer*. Packt, 2018.
- [9] Hamid Jahankhani, editor. *Cyber Security Practitioner’s Guide*. World Scientific, 2019.
- [10] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
- [11] B. Liskov and L. Shrira. Promises: Linguistic support for efficient asynchronous procedure calls in distributed systems. In *Int. Conf. on Programming Language Design and Implementation (SIGPLAN’88)*, pages 260-267, 1988.
- [12] A. Mead. *Learning Node.js Development*. Packt, 2018.
- [13] I. Mitchell and S. Hara. *Blockchain and Clinical Trial - Securing Patient Data*. Advanced Sciences and Technologies for Security Applications. Springer, 2019.
- [14] I. Mitchell and S. Hara. *BMAR - blockchain for medication administration records*. In Jahankhani [13], 2019.

- [15] I. Mitchell, S. Hara, H. Jahankhani, and D. Neilson. Blockchain of custody, boc. [9].
- [16] I. Mitchell, M. Sheriff, and S. Hara. DappER: Decentralised Application for Exam Reviews. 2019.
- [17] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [18] Giang-Truong Nguyen and Kyungbaek Kim. A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, 14(1), 2018.
- [19] D. Parker. *Javascript with Promises*. O'Reilly, 1 edition, 2015.
- [20] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.
- [21] R.L. Rivest. The md5 message-digest algorithm, request for comments (rfc1320). 1992.
- [22] Rogaway and Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. *LNCS Software Encryption*, 2004.
- [23] Scientific Working Group on Digital Evidence (SWDGE). Model standard operation procedures for computer forensics (ver. 3). <https://www.swgde.org/>. [Accessed June 2016].
- [24] Parth Thakkar, Senthil Nathan, and Balaji Vishwanathan. Performance benchmarking and optimizing hyperledger fabric blockchain platform. *arXiv preprint arXiv:1805.11390*, 2018.
- [25] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. Technical report, National Institute of Standards and Technology, 2018.