TAKE-HOME ONLINE EXAMINATIONS APRIL – JUNE 2021

Please read through all instructions carefully before you start your exam

In most cases, the take-home online exam will be available for 23 hours and your answer(s) must be submitted before 9.00am UK time the day after your take-home online exam opens, unless you have been given a different deadline from your School.

Completing your take-home online exam

1. You need to download the question paper and any accompanying documents from Blackboard and your answers can be written in a Word document as you would for coursework (unless you have been given specific instructions from your School).
2. You are advised only to work on your answers for the duration of the time stated on the front page of the take-home online exam paper. You are not expected to work for 23 hours on your answer(s).
3. For some exams a timer will be applied so that, once started, you must submit within the specified time limit. Exams with a time limit will require you to submit either to a Blackboard test or to a Gradescope assignment. These will be clearly identified in Blackboard.
4. For exams which are time-restricted, and where you are required to upload your answers in a file, an extra 30 minutes will be added. This additional time is to allow you to scan any handwritten work and upload your file. Work submitted beyond this 30 minute period will be treated as late, and will not be marked.
5. Please read your exam paper thoroughly before you start to ensure that you understand what you need to do.
6. Do not exceed the specified word limits where they are stated.
7. You should use 12pt font size, Arial and 1.5 line spacing for word processed submissions.
8. Please write your 5-digit anonymous candidate number (from your RISIS exam timetable), module code and the number(s) of the question(s) answered on the top of each piece of work that you submit.
9. Save your work regularly as you are working on it.
10. You are responsible for the content of the work you upload and for the academic integrity of your answer(s).
11. Complete and upload your answer(s) to the submission point(s) in your Blackboard course.
12. You are responsible for organising your time and should aim to submit your answer(s) as early as possible to ensure your work is submitted prior to the deadline specified for your take-home online exam paper.

Full guidance can be found in the Take Home Exams area of this Blackboard course.

Submission

1. Please check the front of your take-home online exam paper and Blackboard for any specific instructions for uploading your work to submission point(s) for each paper.
2. You can submit multiple times for most exams (unless you have been told there is only one submission possible by your School), but you should ensure that your final version is uploaded before the deadline.
3. When submitting to Turnitin the 'submission title' must start with your 5-digit anonymous candidate number, followed by the module code. An example of a submission title is 12345 HS3DR.
4. You are responsible for ensuring that you have uploaded the correct document to the correct submission point. Some exams require submission of answers for different questions to different submission points.
5. You are responsible for ensuring that your file has been uploaded successfully. When you submit to a Turnitin, Blackboard or Gradescope 'variable-length' assignment you will receive an email receipt which you must keep. If you do not get this email receipt your work has not been submitted (check your spam folder).
   You will not receive an email receipt when you submit to a Blackboard Test or Gradescope Online Assignment.
   Please note that the final stage of a Turnitin submission requires you to confirm your submission by clicking 'Confirm'.
6. Please allow yourself plenty of time to upload and submit your answer(s) by the deadline. If you have problems submitting your answer(s) please email your work to take-home-exam@reading.ac.uk as soon as possible.
7. We will not be emailing reminders from the University ahead of exam papers and submission points opening, or non-submissions after the take-home exam submission has closed.
8. Guidance on how to submit files for your exams can be found at https://rdg.ac/takehomeexam

Full guidance can be found in the Take Home Exams area of this Blackboard course.

Where to get support

If you need support during your exam you can contact us on +44 (0) 118 378 7049

For technical issues (Blackboard and IT) you can also raise a ticket via the DTS Self Service Portal.

For other non-technical queries, please check the exams FAQs on Essentials or email take-home-exam@reading.ac.uk. Emails need to be sent from your University email account and you should provide your 5-digit candidate number.

Please note that ‘live’ support is available from 8:00am-5:00pm UK time Monday to Friday and will be available for limited hours 8:00am-9.30am UK time on Saturday morning during the exam period.

DAS registered students

1. If you have been provided with a green sticker, please attach this to the front page of your answer(s), as you would do for coursework submissions.
2. If you have any additional arrangements including extra time, you should consider the necessary requirements prior to the start of your exam and read the advice in the exam FAQs on Essentials.
3. If you still have queries please contact the Disability Advisory Service (DAS) or email take-home-exam@reading.ac.uk. Emails need to be sent from your University email account and you should provide your 5-digit candidate and student number.

IMPORTANT - You must read this before you start your exam

Academic Integrity

We are treating this online examination as a time-limited open assessment. This means that:

1. You are permitted to refer to published materials to aid you in your answers.
2. Published sources must be referenced. This includes all on-line sources.
3. Over-reliance on published sources is considered to be poor academic practice.

Apart from appropriate referencing, you must ensure that:

a. the work you submit is entirely your own;
b. you do not communicate with other students on the topic of this assessment for the whole time the assessment is live;
c. you do not obtain advice or contribution from any third party, including proof-readers, friends, or family members.
d. For advice on academic integrity, you can see the University Library’s Academic Integrity Toolkit.

You should note that:

1. Failure to adhere to these requirements will be considered a breach of the Academic Misconduct regulations (available here), where the offences of cheating, plagiarism, collusion, copying, and commissioning are particularly relevant.
2. Your exam answers will be run through Turnitin, and the usual similarity reports will be available to markers.

Please read and note this statement of originality:

By submitting this work I certify that:

1. **it is my own unaided work;**
2. **the use of material from other sources has been properly and fully acknowledged in the text;**
3. **neither this piece of work nor any part of it has been submitted in connection with another assessment;**
4. **I have read the University's definition of plagiarism, guidance on good academic practice and the guidelines set out above; and**
5. **I will comply with the requirements these place on me.**

I acknowledge the University may use appropriate software to detect similarities with other third-party material, in order to ensure the integrity of the assessment.

I understand that if I do not comply with these requirements the University will take action against me, which if proven and following the proper process may result in failure of the year or part and/or my removal from membership of the University.

With best wishes and good luck for your take-home online exams over the coming period.

Please read the instructions below before you start the exam.

April/May 2021 **CS3BC20 2020/1 A 800**

UNIVERSITY OF READING

BLOCKCHAIN COMPUTING (CS3BC20)

Two hours

Answer **Question 1** and any **TWO** out of THREE remaining Questions.

If a word limit is not specified next to a QUESTION then EACH QUESTION (e.g. Q1, Q2, Q3, etc.) has a word limit of 1000 words.
This limit excludes scanned images of diagrams or hand-written formulas but includes images with hand-written text.

Submit your answers to **EACH QUESTION** SEPARATELY to the relevant submission point on Blackboard.

EACH Question is worth 20 marks.

(YOU MUST ANSWER QUESTION 1)

1. (a) Suppose that it is intended to use Blockchain technology to support the authenticity and traceability checking of goods in the following supply chains:

(i) Authenticated Pure Virgin Olive Oil
(ii) Infection traceable Organic Eggs

For each of the above two supply chains specify the Block data structure in terms of variables that would need to be represented.

(4 marks)

(b) In addition to authenticity, there is a requirement to keep an auditable record of refrigeration in-transit end-to-end as well as the expiry-date (e.g. as for the Pfizer BioNtech Vaccine, or fast perishable food such shellfish), therefore you are required to:

(i) define the block data structure that best supports these additional requirements for the distribution chain of such goods, and
(ii) suggest a blockchain solution stack to enforce a delivery for the vaccine or shellfish with a specified cold temperature maintained throughout transit.

(4 marks)

(c) State and justify the type of Blockchain to be used for each supply chain for cases (a) (i) and (ii) above.

(1 mark)

(d) Justify why Proof-of-Work and Proof-of-Stake Consensus methods should not be expected to be vulnerable to the same type of attacks and describe one type of security threat that the Proof-of-Stake could be exposed to.

(5 marks)

(e) Briefly describe each of 4 distinct routes to a double-spend attack that could be mounted on a blockchain.

(6 marks)

2. (a) Describe any three cyber-attack types to which a smart contract could be vulnerable.

(9 marks)

(b) Describe one design feature which could support post-hoc vulnerability fixing of smart contracts and how this might be implemented despite the immutability of Blockchain.

(3 marks)

(c) Describe an alternative consensus platform that in your view improves upon Proof-of-Work (PoW) with respect to the drawbacks of PoW that you can identify. Explain how such a consensus platform would work.

(3 marks)

(d) Specify the algorithm deployed to ensure the maintenance of blockchain integrity by verifying the authenticity of each block at the node, wallet, transaction and block levels and describe how this is achieved through a system of crypto-hash pointers and digital signatures.

(5 marks)

3. (a) A malicious node wishes to introduce an invalid node into the Blockchain network. With reference to the Byzantine Fault Tolerance capability of the blockchain, explain how this attempt is doomed to fail.

(3 marks)

(b) A malicious actor has managed to steal a large sum of cryptocurrency from the users' wallets by hacking an exchange. The affected Blockchain community has agreed that a rollback should occur so that funds can be returned to their original owners. Explain what happens when a rollback occurs on a blockchain.

(3 marks)

(c) State what ethical and social concerns are associated with rolling back a Blockchain and what the wider implications of the adoption of a rollback might be.

(4 marks)

(d) What alternative mitigation measures may be open to this community in order to avoid a rollback but at the same time ensure that the perpetrators could not benefit from the proceeds of their crime?

(4 marks)

(e) Discuss two major type of threats that could expose the blockchain to the risk of insecure re-centralisations; suggest a possible regulatory measure that may help reduce at least one such source of threat to the blockchain and the cryptocurrencies sector.

(6 marks)

4. (a) Explain the measures taken by:

(i) the Blockchain platform and network, and
(ii) the vendors

to prevent double-spend attacks.

(4 marks)

(b) Person X wishes to share a solution to a puzzle to the Blockchain. If they are the first person to solve the puzzle by publishing the solution to the Blockchain they will win a reward for being first. Therefore, Person X shares their solution with the transaction pool to be published to the Blockchain. However, there is a problem in that, this information is now public before it is has been published to the Blockchain. A malicious miner or observer could steal the solution and undercut the original owner by republishing the transaction with a higher fee, meaning it is published first;

(i) Propose a solution (that can involve smart contracts) that enables Person X to safely share their solution with the transaction pool; with no worry of being **a)** undercut *and/or* **b)** having their information stolen before being included on the Blockchain.

(2 marks)

(ii) Explain the steps whereby your solution could be implemented.

(6 marks)

(c) There exists a regulatory void in which some of the emerging cryptocurrency business models operate. Briefly discuss this by reference to an unethical trading tactic that could occur in cryptocurrency trading and which is illegal in normal stock trading practice.

(4 marks)

(d) Outline the legal and computational challenges that have to be overcome in order for smart contracts to be considered as a valid form of contract.

(4 marks)

(End of Question Paper)