Principles of Decentralized Ledgers
Courseguide 2022

Dr. Arthur Gervais

Part I
Course Layout

The course takes place in the second term — online on Teams (see the link in the Imperial calendar) — over a duration of 9 weeks, with 7 main lectures and 7 supporting/Q&A lectures. The main lectures are pre-recorded, while the supporting/Q&A lectures are scheduled on Fridays 11-13am UK time. The inaugural Q&A lecture is scheduled for Friday, the 21st of January 2021, at the Teams link above. Please do watch the first intro video prior to this first lecture.

The recorded lectures serve to primarily convey the main course contents. You can find these lectures on YouTube (`https://www.youtube.com/playlist?list=PL0a3v6xgsJullbz4uD13nm-U5D_cw0xLh`) as well as on Scientia (`https://scientia.doc.ic.ac.uk/2122/modules/70066`) and Panopto for your convenience. The pre-recorded lectures are divided into digestible bits on the order of 5-15 minutes each. The supporting lectures serve to discuss, for example about smart contract programming, relevant scientific papers, advances on course works as well as to elaborate and repeat on the contents provided within the main lecture.

1 Schedule

You can find the tentative course schedule in Table 1.

2 Grading Scheme

We plan the following course works, exam and grading scheme for this year's course.

Blockchain Workbench 10% of the grade

Blockchain dApp 10% of the grade

Exam 80% of the grade

21.01	**Blockchain Introduction** — Q&A Please watch lecture 1 until then.
28.01	**Proof of Work** — Q&A Please watch lecture 2 until then. Coursework 1 start: Blockchain Workbench
04.02	**Smart Contracts** — Q&A Please watch lecture 3 until then. Paper Reading/Presentation by lecturer
11.02	**Network** — Q&A Please watch lecture 4 until then. Blockchain Exam Exercises Due date for Coursework 1 Coursework 2 starts: Decentralized Application
18.02	**Security** — Q&A Please watch lecture 5 until then. Paper Reading/Presentation by lecturer
25.02	**Scaling** — Q&A Please watch lecture 6 until then. Previous Exercise Exam
04.03	**Privacy** — Q&A Please watch lecture 7 until then. Due date Coursework 2
11.03	Summary Revision / Q&A (Optional)

Table 1: Tentative Course Schedule 2022.

Part II
Course works

This course will have two graded course works, (i) the blockchain workbench, and (ii) completing a decentralized application.

3 Blockchain Workbench

To complement the lectures, we will work through the blockchain workbench (`https://blockchainworkbench.com/`). The blockchain workbench covers the blockchain basics and allows learning and practice the development of solidity based smart contracts. You will be expected to walk through the exercises of the workbench and share the resulting completion data blob upon finalization of the workbench.

3.1 Coursework Instructions

Important: Please do all your coursework activity in one browser session. If you change the browser, or delete your cache/history, you'll delete your progress. If things don't work well (most likely due to some other settings/browser plugins), try to use incognito mode, but do not close your incognito window before you are done! When you are done, you can download course blockchaincoursework file and upload on Cate.

1. Please visit `https://www.blockchainworkbench.com/toc`
2. Enter your CID and click on the right button with the two arrows to record your CID locally. The website will show that it saved your CID.
3. Please visit `https://www.blockchainworkbench.com`
4. Click on "Start!".
5. Follow and complete the exercises until and including "Pichu Muffin Pilots" in the section "Types".
6. Please visit again `https://www.blockchainworkbench.com/toc`
7. Download your progress.
8. Upload your progress on Cate.

Grading: We'll count the number of exercises that you successfully completed and will adjust your grade proportionally.

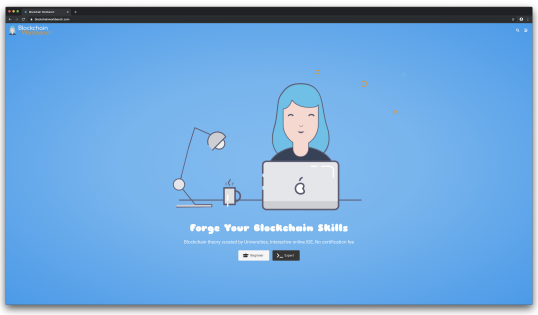

Figure 1: Blockchain Workbench landing page. Proceed as "Beginner".

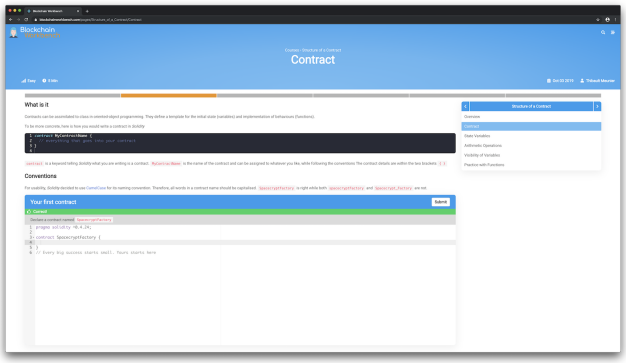

Figure 2: Smart contract IDE integrated into the web interface with editor, deploy and test scripts.

4 Decentralised Application

For the second coursework, we will give you a decentralised application that is not yet functional and needs to be completed. You are expected to become more familiar and put into practice the development of a smart contract by completing missing functions within this application. Besides the tutorials of the blockchain workbench, you might find the following resource helpful: `https://docs.soliditylang.org/en/v0.8.0/`.

4.1 Coursework Instructions

The full coursework specification (including grading scheme) can be found here: `https://github.com/Research-Imperium/COMP70017-CW2-2022`**. Once you are done, please upload the entire repository on Cate.**

5 Paper Reading/Presentation

The blockchain field is only 10 years old, and heavily driven by academic research results. To stay at the edge of this nascent technology we will review/discuss several academic, peer-reviewed papers (tentative list):

- Bitcoin: A Peer-to-Peer Electronic Cash System by Sathoshi Nakamoto (`https://bitcoin.org/bitcoin.pdf`)
- On the security and performance of proof of work blockchains by Gervais et al. (`https://eprint.iacr.org/2016/555.pdf`)
- Majority Is Not Enough: Bitcoin Mining Is Vulnerable by Eyal and Sirer (`https://link.springer.com/chapter/10.1007/978-3-662-45472-5_28`).
- Do you need a Blockchain? by Gervais et al. (`http://doyouneedablockchain.com/`)

Part III
Exam

The exam will cover the topics and problems discussed within the lectures (i.e. not necessarily capture all contents of the papers that are being discussed/read, but the parts that are discussed within the lecture). We will have two lectures where we will work on (i) generic exam questions, and (ii) an exam from the previous years.

Part IV
Administrative Comments

5.1 External Students – Registration for DoC Courses

1. Apply at: `https://dbc.doc.ic.ac.uk/externalreg/`
2. Then,
   - Your department's endorser will approve/reject your application
3. If approved,
   - DoC's External Student Liaison will approve/reject your application
4. If approved (again!),

- Students will get access to DoC resources (DoC account, CATE, materials, ...)
- No access after a few days? Check status of approval and contact relevant person(s)

Key Dates

- Exams for DoC $3^{rd}/4^{th}$ yr. courses take place at the end of the Term in which the course is taught
- Registration for exams opens end January

If in doubt, read the guidelines available at the link above :)