Board of Studies

Course Proposal Template

PROPOSED COURSE TITLE: Blockchain and Distributed Ledgers

PROPOSER(S): Aggelos Kiayias

DATE: March, 8 2017

SUMMARY

This template contains the following sections, which should be prepared roughly in the order in which they appear (to avoid spending too much time on preparation of proposals that are unlikely to be approved):

[Guidance in square brackets below each item. Please also refer to the guidance for new course proposals at http://www.inf.ed.ac.uk/student-services/committees/board-of-studies/course-proposal-guidelines. Examples of previous course proposal submissions are available on the past meetings page http://web.inf.ed.ac.uk/infweb/admin/committees/bos/meetings-directory.]

SECTION 1 – CASE FOR SUPPORT

[This section should summarise why the new course is needed, how it fits with the existing course portfolio, the curricula of our Degree Programmes, and delivery of teaching for the different years it would affect.]

1a. Overall contribution to teaching portfolio

[Explain what motivates the course proposal, e.g. an emergent or maturing research area, a previous course having become outdated or inappropriate in other ways, novel research activity or newly acquired expertise in the School, offerings of our competitors.]

Blockchain technology and distributed ledgers have been hailed as a turning point in scaling information technology services at a global level. Although the digital currency Bitcoin is the best-known blockchain application today, the technology is set to play a much broader role in cyber security. This course is an introduction to the design and analysis of blockchain systems. It is expected to have good synergy with the Blockchain Technology Laboratory that was created recently in the school of Informatics and there will be ample opportunities for interested students to interact with researchers at the lab that are working on actual blockchain systems. There are successful courses taught at a similar level in Stanford University (https://crypto.stanford.edu/cs251/), UC Berkeley (https://blockchain.berkeley.edu/decal/), UC David (https://rylanschaeffer.github.io/resources/198FCourseSyllabus.pdf) as well as a very successful online course created by Princeton University (https://www.coursera.org/learn/cryptocurrency).

1b. Target audience and expected demand

[Describe the type of student the course would appeal to in terms of background, level of ability, and interests, and the expected class size for the course based on anticipated demand. A good justification would include some evidence, e.g. by referring to projects in an area, class sizes in similar courses, employer demand for the skills taught in the course, etc.]

The course is targeted towards fourth year students as well as first year graduate students. The course is meant to be taught in parallel to the Introduction to Modern Cryptography course of the same level (INFR11131) at least every other year (with the latter course as a prerequisite or co-requisite). As in the case of INFR11131, it is recommended that students have taken a class in algorithms and/or data structures. It is also recommended that the students have a good understanding of discrete mathematics, probability and programming. There is currently is a high demand for computer science graduates with a good understanding of cryptography and its applications and blockchain technology is an excellent application domain to understand how cryptography can be used to solve real world problems in cyber security. The course is also directed to those students that have attended Computer Security (INFR09025), however students are able to take it without attending computer security.

1c. Relation to existing curriculum

[This section should describe how the proposed course relates to existing courses, programmes, years of study, and specialisms. Every new course should make an important contribution to the delivery of our Degree Programmes, which are described at http://www.drps.ed.ac.uk/15-16/dpt/drps_inf.htm.

Please name the Programmes the course will contribute to, and justify its contribution in relation to courses already available within those programmes. For courses available to MSc students, describe which specialism(s) the course should be listed under (see http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2015/programme-guide/specialist-areas), and what its significance for the specialism would be. Comment on the fit of the proposed course with the structure of academic years for which it should be offered. This is described in the Year Guides linked from http://web.inf.ed.ac.uk/infweb/student-services/ito/students.]

The course contributes to the programmes of Computer Science and Computer Science and Mathematics as well as the Master of Informatics (MInf). The students of Computer Science and Physics can also benefit from it. At the graduate level, the course should be listed under the cybersecurity and privacy specialist area. Its significance for cybersecurity and privacy stems from the fact that it illustrates how concepts studied in other courses such as Introduction to Modern Cryptography (INFR11131) but also Computer Security (INFR09025) can be applied in a real world setting.

1d. Resources

[While course approvals do not anticipate the School's decision that a course will actually be taught in any given year, it is important to describe what resources would be required if it were run. Please describe how much lecturing, tutoring, exam preparation and marking effort will be required in steady state, and any additional resources that will be required to set the course up for the first time. Please make sure that you provide estimates relative to class size if there are natural limits to its scalability (e.g. due to equipment or space requirements). Describe the profile of the course team, including lecturer, tutors, markers, and their required background. Where possible, identify a set of specific lecturers who have confirmed that they would either like to teach this course apart from the proposer, or who could teach the course in principle. It is useful to include ideas and suggestions for potential teaching duty re-allocation (e.g. through course sharing, discontinuation of an existing course, voluntary teaching over and above normal teaching duties) to be taken into account when resourcing decisions are made.]

This is a new course that I have assembled this year. No tutoring is required. A grader will be needed to assist with grading the three courseworks. In terms of staff, I will be able to teach it at least every other year. We are hiring now in security and privacy and I anticipate that we will have at least one more faculty member either capable of teaching this course or teaching the Introduction to Modern Cryptography and thus the current proposal has the potential to become a regular offering on a yearly basis.

SECTION 2 – COURSE DESCRIPTOR

[This is the official course descriptor that will be published by the University and serves as the authoritative source of information about the course for student via DRPS and PATH. Current course descriptions in the EUCLID Course Catalogue are available at www.euclid.ed.ac.uk under 'DPTs and Courses', searching for courses beginning 'INFR'*]*

2a. Course Title *[Name of the course.]*:

Blockchains and Distributed Ledgers

2b. SCQF Credit Points:

[The Scottish Credit and Qualifications Framework specifies where each training component provided by educational institutions fits into the national education system. Credit points per course are normally 10 or 20, and a student normally enrols for 60 credits per semester. For those familiar with the ECTS system, one ECTS credit is equivalent to 2 SCQF credits. See also http://www.scqf.org.uk/The%20Framework/Credit%20Points.]

10

SCQF Credit Level:

[These levels correspond to different levels of skills and outcomes, see http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf At University level, Year 1/2 courses are normally level 8, Year 3 can be level 9 or 10, Year 4 10 or 11, and Year 5/MSc have to be level 11. MSc programmes may permit a small number (up to 30 credits overall) of level 9 or 10 courses.]

11

Normal Year Taken: 1/2/3/4/5/MSc

[While a course may be available for more than one year, this should specify when it is normally taken by a student. "5" here indicates the fifth year of undergraduate Masters programmes such as MInf.]

4

Also available in years: 1/2/3/4/5/MSc

Different options are possible depending on the choice of SCQF Credit Level above: for level 9, you should specify if the course is for 3rd year undergraduates only, or also open to MSc students (default); for level 10, you should specify if the course is available to 3rd year and 4th year undergraduates (default), 4th year undergraduates only, and whether it should be open to MSc students; for level 11, a course can be available to 4th and 5th year undergraduates and MSc students (default), to 5th year undergraduates and MSc students, or to MSc students only]

5/MSc

2c. Subject Area and Specialism Classification:

[Any combination of Computer Science, Artificial Intelligence, Software Engineering and/or Cognitive Science as appropriate. For courses available to MSc students, please also specify the relevant MSc specialist area (to be found in the online MSc Year Guide at http://web.inf.ed.ac.uk/infweb/student-services/ito/students/taught-msc-2015/programme-guide/specialist-areas), distinguishing between whether the course should be considered as "core" or "optional" for the respective specialist area.]

Computer Science, Specialist Areas: Cyber Security and Privacy

Appropriate/Important for the Following Degree Programmes:

[Please check against programmes from http://www.drps.ed.ac.uk/15-16/dpt/drps_inf.htm to determine any specific programmes for which the course would be relevant (in many cases, information about the Subject Area classification above will be sufficient and specific programmes do not have to be specified). Some courses may be specifically designed for non-Informatics students or with students with a specific profile as a potential audience, please describe this here if appropriate.]

Computer Science Computer Science and Mathematics Computer Science and Physics Master of Informatics Also suitable for Mathematics majors.

Timetabling Information:

[Provide details on the semester the course should be offered in, specifying any timetabling constraints to be considered (e.g. overlap of popular combinations, other specialism courses, external courses etc).]

To be offered in the first semester of the fourth year. It naturally follows Computer Security offered in the third year and also facilitates Secure Programming to be taken in the second semester of the fourth year. It is meant to be taught in parallel to Introduction to Modern Cryptography.

2d. Summary Course Description:

[Provide a brief official description of the course, around 100 words. This should be worded in a student-friendly way, it is the part of the descriptor a student is most likely to read.]

Blockchain technology and distributed ledgers have been hailed as a turning point in scaling information technology services at a global level. Although the digital currency Bitcoin is the best-known blockchain application today, the technology is set to play a much broader role in cyber security and information technology. This course is an introduction to the design and analysis of blockchain systems and distributed ledgers and is meant to be taught in parallel to the Introduction to Modern Cryptography course of the same level (INFR11131) every other year (with the latter course as a prerequisite or co-requisite).

Course Description:

[Provide an academic description, an outline of the content covered by the course and a description of the learning experience students can expect to get. See guidance notes at: http://www.studentsystems.is.ed.ac.uk/staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

Designing blockchain and distributed ledger systems relates to the areas of cryptography and distributed systems. A blockchain protocol can be used to build a distributed ledger that maintains some form of record of transactions in a way that the data maintained are immutable, extendable and available to any authorized party that requests them. Students will understand how blockchain protocols work, what are their underlying assumptions and what are the security guarantees that they offer. They will also become familiar with various applications of blockchain protocols and distributed ledgers in realizing cryptocurrencies, object registries, inventories and smart contracts. Various cryptographic techniques for safely data processing information related to ledgers will also be introduced including secure multiparty computation and zero-knowledge protocols.

Pre-Requisite Courses:

[Specify any courses that a student must have taken to be permitted to take this course. Pre-requisites listed in this section can only be waived by special permission from the School's Curriculum Approval Officer, so they should be treated as "must-have". By default, you may assume that any student who will register for the course has taken those courses compulsory for the degree for which the course is listed in previous years. Please include the FULL course name and course code].

Recommended to have Computer Security INFR10058, Algorithms and Data Structures, INFR09006, INFR10052.

Co-Requisite Courses:

[Specify any courses that should be taken in parallel with the existing course. Note that this leads to a timetabling constraint that should be mentioned elsewhere in the proposal. Please include the FULL course name and course code].

Introduction to Modern Cryptography (INFR11131).

Prohibited Combinations:

[Specify any courses that should not be taken in combination with the proposed course. Please include the FULL course name and course code].

none

Other Requirements:

[Please list any further background students should have, including, for example, mathematical skills, programming ability, experimentation/lab experience, etc. It is important to consider that unless there are formal prerequisites for participation in a course, other Schools can register their students onto our courses, so it is important to be clear in this section. If you want to only permit this by special permission, a statement like "Successful completion of Year X of an Informatics Single or Combined Honours Degree, or equivalent by permission of the School." can be included.]

Basic understanding of probability. Discrete mathematics. Programming.

Available to Visiting Students: Yes/No

[Provide a justification if the answer is No.]

Yes.

2e. Summary of Intended Learning Outcomes (MAXIMUM OF 5):

[List the learning outcomes of the course, emphasising what the impact of the course will be on an individual who successfully completes it, rather than the activity that will lead to this outcome. Further guidance is available from https://canvas.instructure.com/courses/801386/files/24062695]

On completion of this course, the student will be able to

1. Understand what is a blockchain and a distributed ledger

2. Develop or extend the ability to think critically about cybersecurity

3. Appreciate the challenges of scaling information technology services across organizational barriers and at a global level.

4. Enhance the understanding of basic cryptographic primitives like hash functions and digital signatures

Assessment Information

[Provide a description of all types of assessment that will be used in the course (e.g. written exam, oral presentation, essay, programming practical, etc) and how each of them will assess the intended learning outcomes listed above. Where coursework involves group work, it is important to remember that every student has to be assessed individually for their contribution to any jointly produced piece of work. Please include any minimum requirements for assessment components e.g. student must pass all individual pieces of assessment as well as course overall].

30% of the assessment will be on an assigned coursework aiming at objectives 1,2,3,4 above. The rest 70% will be on a final examination.

Assessment Weightings:

Written Examination: 70%

Practical Examination: 0%

Coursework: 30%

Time spend on assignments:

[Weightings up to a 70/30 split between exam and coursework are considered standard, any higher coursework percentage requires a specific justification. The general expectation is that a 10-point course will have an 80/20 split and include the equivalent of one 20-hour coursework assignment (although this can be split into several smaller pieces of coursework. The Practical Examination category should be used for courses with programming exams. You should not expect that during term time a student will have more than 2-4 hours to spend on a single assignment for a course per week. Please note that it is possible, and in many cases desirable, to include formative assignments which are not formally assessed but submitted for feedback, often in combination with peer assessment.]

The coursework that will be graded corresponds to a total of 30 hours of work. A total of three assignments will be given and each one will require approximately 10 hours of work. Other assignments will be provided but not counted towards the final grade.

Academic description:

[A more technical summary of the course aims and contents. May include terminology and technical content that might be more relevant to colleagues and administrators than to students.]

The concept of blockchain will be covered in detail together with all related cryptographic techniques. The underlying cryptographic primitives that are necessary to design blockchain systems will be covered including proofs of work, digital signatures and hash functions. The definition of a robust transaction ledger from a security modeling point of view. Properties such as persistence of transactions, liveness of the ledger considered in the presence of an adversary that wishes to subvert them. The assumptions under which blockchain protocols can provide their security guarantees. Applications such as cryptocurrencies, inventories, name registries, reputation systems. Game theoretic approaches to analysis of blockchain protocols. Advanced cryptographic methods that are important for ledger systems such as secure multiparty computation protocols and zero-knowledge proofs for privacy preserving ledger operations.

Syllabus:

[Provide a more detailed description of the contents of the course, e.g. a list of bullet points roughly corresponding to the topics covered in each individual lecture/tutorial/coursework. The description should not exceed 500 words but should be detailed enough to allow a student to have a good idea of what material will be covered in the course. Please keep in mind that this needs to be flexible enough to allow for minor changes from year to year without requiring new course approval each time.]

1. Introduction to blockchain. What is a distributed ledger. Transactions. Digital Signatures.
2. The consensus layer. Basic Properties. Proof of Work.
3. Robust Transaction Ledgers. Properties and Objectives. Permissioned, permissionless ledgers.
4. Privacy Issues. Anonymity, Pseudonymity, Unlinkability. Zero-Knowledge Proofs.
5. Scalability Issues. Byzantine agreement protocols.
6. Blockchain as a platform. Smart Contracts.
7. Secure multiparty computation techniques and their application to blockchain protocols.
8. Alternative techniques to proof of work for blockchain protocols, proof of stake/space.
9. Game theoretic analysis of blockchain protocols.
10. Name and object registries. Reputation systems. Policy issues related to blockchain.

Relevant QAA Computing Curriculum Sections:

[Please see http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-consultation-15.pdf to check which section the course fits into.]

I230: Systems analysis & design

Graduate Attributes, Personal and Professional skills:

[This field should be used to describe the contribution made to the development of a student's personal and professional attributes and skills as a result of studying this course – i.e. the generic and transferable skills beyond the subject of study itself. Reference in particular should be made to SCQF learning characteristics at the correct level http://www.sqa.org.uk/files_ccc/SCQF-LevelDescriptors.pdf].

Characteristic 1, Level 5.

Characteristic 2, Level 10.

Characteristic 3, Level 5.

Characteristic 4, Level 5.

Characteristic 5, Level 5.

*[Provide a list of relevant readings. See also remarks under **3d**.]*

Breakdown of Learning and Teaching Activities:

[Total number of lecture hours and tutorial hours, with hours for coursework assignments.]

[The breakdown of learning and teaching activities should only include contact hours with the students; everything else should be accounted for in the Directed Learning and Independent Learning hours.

The total being 10 x course credits. Assume 10 weeks of lectures slots and 10 weeks of tutorials, though not all of these need to be filled with actual contact hours. As a guideline, if a 10-pt course has 20 lecture slots in principle, around 15 of these should be filled with examinable material; the rest should be used for guest lectures, revision sessions, introductions to assignments, etc. Additional categories of learning and teaching activities are available, a full list can be found at:

http://www.euclid.ed.ac.uk/Staff/Support/User_Guides/CCAM/Teaching_Learning.htm]

Lecture Hours: 18 hours

Seminar/Tutorial Hours: 0 hours

Supervise practical/Workshop/Studio hours: 0 hours

Summative assessment hours: 15 hours

Feedback/Feedforward hours: 2 hours

Directed Learning and Independent Learning hours: 55 hours

Total hours: 90 hours

You may also find the guidance on 'Total Contact Teaching Hours' and 'Examination & Assessment Information' at:
http://www.studentsystems.ed.ac.uk/Staff/Support/User_Guides/CCAM/CCAM_Information_Captured.html

Keywords:

[A list of searchable keywords.]

Cryptography, bitcoin, cyber security.

SECTION 3 - COURSE MATERIALS

3a. Sample exam question(s)

[Sample exam questions with model answers to the individual questions are required for new courses. A justification of the exam format should be provided where the suggested format non-standard. The online list of past exam papers gives an idea of what exam formats are most commonly used and which alternative formats have been http://www.inf.ed.ac.uk/teaching/exam_papers/.]

The exam will be multiple choice. Example question : Mina, a malicious miner, prior to including a transaction to the current block she is preparing, modifies the script so that the transaction output matches her bitcoin account.

A. The block will become invalid because no proof of work can be produced.
B. The transaction will become invalid as other miners will notice Mina's account.
C. The blockchain will become invalid because Mina's received more bitcoin than originally intended.
D. The resulting transaction will become invalid because the sender's signature will be invalid. (Correct answer)

3b. Sample coursework specification

[Provide a description of a possible assignment with an estimate of effort against each sub-task and a description of marking criteria.]

Example question. *Assuming that the adversary completely controls the network and relative hashing power α, design a selfish mining strategy that obtains a fraction of α / (1-α) rewards from the blockchain.*

Sub-task 1 : description of the algorithm. Effort requires review selfish mining strategies, suggest algorithm. (4 hours).

Sub-task 2 : analyze the performance of the algorithm in terms of number of blocks. Argue that in a chain of *n* blocks a fraction of $\alpha / (1-\alpha)$ blocks are provided by the adversary. Revisit algorithm to improve as needed. (6 hours).

3c. Sample tutorial/lab sheet questions

[Provide a list of tutorial questions and answers and/or samples of lab sheets.]

None

3d. Any other relevant materials

[Include anything else that is relevant, possibly in the form of links. If you do not want to specify a set of concrete readings for the official course descriptor, please list examples here.]

Satoshi Nakamoto. Bitcoin white paper. https://bitcoin.org/bitcoin.pdf

GKL14 - The backbone paper. Analysis of the bitcoin protocol.
https://eprint.iacr.org/2014/765.pdf

SECTION 4 - COURSE MANAGEMENT

4a. Course information and publicity

[Describe what information will be provided at the start of the academic year in which format, how and where the course will be advertised, what materials will be made available online and when they will be finalised. Please note that University and School policies require that all course information is available at the start of the academic year including all teaching materials and lecture slides.]

1. Syllabus.
2. Lecture notes. Slides.
3. Description of marking scheme.
4. Sample homework.

4b. Feedback

[Provide details on feedback arrangements for the course. This includes when and how course feedback is solicited from the class and responded to, what feedback will be provided on assessment (coursework and exams) within what timeframe, and what opportunities students will be given to respond to feedback.

The University is committed to a baseline of principles regarding feedback that we have to implement at every level, these are described at http://www.docs.sasg.ed.ac.uk/AcademicServices/Policies/Feedback_Standards_Guiding_Principles.pdf.

Further guidance is available from http://www.enhancingfeedback.ed.ac.uk/staff.html.]

Feedback from the students will be solicited on the clarity of the slides, the suitability of the assignments and the general presentation of the course material.

4c. Management of teaching delivery

[Provide details on responsibilities of each course staff member, how the lecturer will recruit, train, and supervise other course staff, what forms of communication with the class will be used, how required equipment will be procured and maintained. Include information about what support will be required for this from other parties, e.g. colleagues or the Informatics Teaching Organisation.]

The marker will be trained by the instructor. The instructor will be provided a detailed marking rubric.

SECTION 5 - COMMENTS

[This section summarises comments received from relevant individuals prior to proposing the course. If you have not discussed this proposal with others please note this].

Nothing significant to mention.

5a. Year Organiser Comments

[Year Organisers are responsible for maintaining the official Year Guides for every year of study, which, among other things, provide guidance on available course choices and specialist areas. The Year Organisers of all years for which the course will be offered should be consulted on the appropriateness and relevance on the course. Issues to consider here include balance of course offerings across semesters, subject areas, and credit levels, timetabling implications, fit into the administrative structures used in delivering that year.]

5b. BoS Academic Secretary

[Any proposal has to be checked by the Secretary of the Board of Studies prior to discussion at the actual Board meeting. This is a placeholder for their comments, mainly on the formal quality of the content provided above.]