School of Informatics Teaching Course Proposal Form

This version was generated **February 21, 2017**. User 'akiayias@inf.ed.ac.uk' verified.

Proposal

Course Name:	Blockchains and Distributed Ledgers
Proposer's Name:	Aggelos Kiayias
Email Address:	akiayias@inf.ed.ac.uk
Course Year:	4
Names of any courses that this new course replaces :	

Course Outline

Course Level:	11
Course Points:	10
Subject area:	Informatics
Programme Collections:	

Teaching / Assessment

Number of Lectures:	20
Number of Tutorials or Lab Sessions:	0
Identified Pre-requisite Courses:	Recommended (INFR10058) AND (INFR09006) OR (INFR10052)
Identified Co-requisite Courses:	INFR11131
Identified Prohibited Combinations:	

Assessment Weightings:

Written Examination:	70%
Assessed Coursework:	30%
Oral Presentations:	0%

Description of Nature of Assessment:

Assessed coursework covering objectives 1-2-3-4 stated above.

Course Details

Brief Course Description:

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 innovation. 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).

The concept of blockchain will be covered in detail together with the supporting cryptographic technology. Questions that will be covered is why it works and what problems can it solve. The lectures will be as follows. 1. Introduction to blockchain. What is a ledger. 2. Transactions. Digital Signatures. 3. The consensus layer. Basic Properties. Proof of Work. 4. Robust Transaction Ledgers. 5. Privacy Issues in the blockchain. 6. Scalability Issues in blockchain systems. 7. Smart Contracts. 8. Proof of stake ledgers. 9. Policy issues related to blockchain. 10. Blockchain as a platform.

Detailed list of Learning Objectives:

1. Understand what is a distributed ledger 2. Develop or extend the ability to think critically about cybersecurity 3. Appreciate the challenges of scaling information technology services at a global level 4. Enhance the understanding of basic cryptographic primitives like hash functions and digital signatures

Syllabus Information:

-

Recommended Reading List:

Bitcoin and cryptocurrency technologies, by Arvind Narayanan (Author), Joseph Bonneau (Author), Edward Felten (Author), Andrew Miller (Author), Steven Goldfeder (Author), Princeton University Press (July 19, 2016). http://bitcoinbook.cs.princeton.edu

The Bitcoin Backbone Protocol: Analysis and Applications, Juan Garay and Aggelos Kiayias and Nikos Leonardos, https://eprint.iacr.org/2014/765

Any additional case for support information: