H9CB: Cryptography and Blockchain

Module Code:	H9CB
Long Title	Cryptography and Blockchain APPROVED
Title	Cryptography and Blockchain
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Arghir Moldovan
Module Author:	Andrea Del Campo Dugova
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Research historical, current, and future trends in cryptography.
LO2	Compare, contrast, and account for the cryptographic theories, principles and techniques used to establish security properties.
LO3	Analyse, choose, and assess existing methods for cryptography and reflect upon the limits and applicability of such methods.
LO4	Investigate Blockchain Technologies, Core Components and current state-of-the-art use cases while demonstrating a concise understanding of Blockchain and Distributed Ledger technologies with corresponding impacts on existing processes and industries.
LO5	Appraise the variations in protocols, challenges and ongoing disruptive nature of Blockchain and Distributed Ledger Technologies, including ethical issues and adoption.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9CB: Cryptography and Blockchain

Module Content & Assessment

Indicative Content
Introduction and History • Types of Cryptography • Classical encryption schemes and their inadequacies • Principles of Modern Cryptography • Perfect Secrecy
Mathematical Preliminaries • Probability • Number Theory • Statistics
Computational Security • One-time Pad • Computational Secrecy • Pseudo Randomness • Stream Ciphers
Block Ciphers • Definition • Types such as S-DES, DES and AES • Multiple Encryption • Mode of Operations (ECB, CBC, CFB, OFB, CTR)
Public Key Cryptography • Public Key Encryption • Digital Signature • RSA-Based Public-Key Encryption • Diffie-Hellman Key Exchange • Public Key Infrastructure (PKI)
Hash Functions • Hash functions • Application of Hash Functions in Public Key cryptography
Foundation of Blockchain Technologies • The History of Blockchain and Cryptocurrencies • Types of Blockchain • Blockchain Stack and Core Components
Blockchain Management • Decentralization • Consensus Mechanisms • DLT - Distributed Ledger Technology • Storing and Using Cryptocurrencies • Smart Contracts
Implementations • Existing and Emerging Use Cases • Evolution of Thus Far (BitCoin, HyperLedger, and Ethereum)
Use Cases and Legal Aspects • Current Use cases of Blockchain • Legal Aspects within the Public Sector
Trend & Future • Quantum Cryptography • The future of Blockchain • Open Problems
Revision Revision

Assessment Breakdown	%
Coursework	40.00%
End of Module Assessment	60.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	Continuous Assessment	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,2
Non-Marked:	No		

Assessment Description:
In class test where students are asked to answer a number of questions.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	60
Assessment Date:	End-of-Semester	**Outcome addressed:**	3,4,5
Non-Marked:	No		

Assessment Description:
The terminal examination will assess the learning outcomes requiring a critical understanding of the concepts related to Cryptography and Blockchain.

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

Reassessment Description
The reassessment strategy for this module will consist of a terminal examination that will assess all learning outcomes.

H9CB: Cryptography and Blockchain

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

Jonathan Katz,Yehuda Lindell. (2020), Introduction to Modern Cryptography, 3rd Edition. Chapman and Hall/CRC, [ISBN: 978-0815354369].

William Stallings. (2020), Cryptography and Network Security: Principles and Practice, 8th Edition. Pearson, [ISBN: 978-0135764268].

Daniel Drescher. (2017), Blockchain Basics: A Non-Technical Introduction in 25 Steps, 1st Edition. Apress, p.255, [ISBN: 978-1484226032].

Supplementary Book Resources

Andreas M. Antonopoulos. (2016), Mastering Bitcoin: Programming the Open Blockchain, 2nd Edition. O'Reilly Media, p.330, [ISBN: 978-1491954386].

Andreas M. Antonopoulos,Gavin Wood. (2018), Mastering Ethereum: Building Smart Contracts and DApps, 1st Edition. O'Reilly Media, p.384, [ISBN: 978-1491971949].

This module does not have any article/paper resources

Other Resources

[Website], Ganache, http://truffleframework.com/ganache

Discussion Note:	