Subject Description Form

Subject Code	COMP5566
Subject Title	Blockchain and Smart Contract Security
Credit Value	3
Level	5
Pre-requisite	COMP5521 Distributed Ledger Technology, Cryptocurrency and E-Payment & COMP5565 Decentralized Apps Fundamentals and Development
Objectives	To equip students with a fundamental understanding of blockchain and smart contract security and practical skills in handling security issues in blockchain and smart contracts. The objectives of this subject are to equip students to: 1. describe the concepts and principles of blockchain and smart contract security; 2. understand the security architectures and threat models of blockchain and smart contracts; 3. analyse the threats to popular blockchain systems and their smart contracts; 4. develop practical skills to detect attacks on and assess the security risk of popular blockchain systems and their smart contracts.
Intended Learning Outcomes *(Note 1)*	Upon completion of the subject, students will be able to: <u>Professional/academic knowledge and skills</u> a) understand the security architectures and threat models of general blockchain and smart contract; b) explain the security mechanisms adopted by popular blockchain systems. c) identify major security threats to popular blockchain systems. d) analyse the security issues in smart contracts and Decentralised applications (DApp) running on popular blockchain systems. <u>Attributes for all-roundedness</u> e) acquire critical thinking and analytical skills, and improve technical writing as well as presentation skills.

<table>
<tr>
<td>Subject Synopsis/ Indicative Syllabus
(Note 2)</td>
<td>
<table>
<tr><th>Topic</th><th>Duration of Lectures</th></tr>
<tr><td>1. Overview of blockchain security
The security architecture of popular blockchain systems, security of keys and wallets, access control, node security</td><td>4.5</td></tr>
<tr><td>2. Network-Level Vulnerabilities and Attacks
Peer-to-peer protocols used by popular blockchain systems like Bitcoin, Ethereum, etc. and the relevant attacks and defence mechanisms, such as Eclipse attack, routing attack, Denial of Service attacks, etc.</td><td>4.5</td></tr>
<tr><td>3. Security of consensus protocols used by popular blockchain systems
Popular consensus protocols, such as Proof of Work, Proof of Stake, Delegated Proof of Stake, Raft, etc. and the corresponding attack and defense strategies, such as 51% attack, selfish mining attack, etc.</td><td>6</td></tr>
<tr><td>4. Smart Contract Security
Security of script used in Bitcoin, security of smart contracts of Ethereum, security of chaincode of Hyperledger Fabric, security of other kinds of smart contracts and the corresponding solutions.</td><td>15</td></tr>
<tr><td>5. Security of Decentralised Applications
Architecture of decentralised applications (DApps), attacks on DApps and the defence strategies.</td><td>4.5</td></tr>
<tr><td>6. Security of oracle and cross-chain systems
Architectures of popular oracle and cross-chain systems, security threats to them and the defense mechanisms</td><td>4.5</td></tr>
<tr><td>Total</td><td>39</td></tr>
</table>
</td>
</tr>
<tr>
<td>Teaching/Learning Methodology
(Note 3)</td>
<td>The course will be delivered as a combination of lectures, tutorials, labs, workshops, and a class project. The course will emphasise both the principles and practices of blockchain and smart contract security. The principles will be covered mainly through the lectures and the tutorials, whereas the practice aspects will be taught through labs and workshops. The class project will help students reinforce what they have learnt, including both principles and practical skills.</td>
</tr>
</table>

Assessment Methods in Alignment with Intended Learning Outcomes

(Note 4)

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)					
		a	b	c	d	e	
1. Assignments	15%	√	√	√	√	√	
2. Class project	15%	√	√	√	√	√	
3. Test(s)	25%	√	√	√	√	√	
4. Examination	45%	√	√	√	√	√	
Total	100 %						

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

Assignment(s): assessment of the studies with respect to the understanding of the relevant subject matters, including the principles, methodologies, and techniques by proving answers to the assignment questions.

Class project: assessment of the ability to solve real problems by using learned techniques and developing practical solutions.

Test(s): assessment of the level of comprehension of core concepts and the ability to apply these concepts to analyze potential threats and solutions in blockchain systems by the time of the mid-term test(s).

Examination: assessment of the overall performance by exam.

Student Study Effort Expected		
	Class contact:	
	▪ Lecture	26 Hrs.
	▪ Tutorial/Lab/Workshop	13 Hrs.
	Other student study effort:	
	▪ Assignment + Term project	35 Hrs.
	▪ Self-study + Examination preparation	48 Hrs.
	Total student study effort	122 Hrs.

Reading List and References	1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press 2016 2. Andreas M. Antonopoulos and Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media; 2018. 3. Elli Androulaki, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, Proceedings of EuroSys'18. 4. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 3rd edition, 2020 5. William Stallings, Cryptography and Network Security: Principles and Practice, 5th edition, Prentice Hall, 2010. 6. Proceedings of IEEE Symposium on Security and Privacy 7. Proceedings of USENIX Security Symposium 8. Proceedings of ISOC Network and Distributed System Security Symposium 9. Proceedings of ACM Conference on Computer and Communications Security 10. Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks 11. Proceedings of Annual Computer Security Applications Conference 12. Proceedings of European Symposium on Research in Computer Security 13. Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses