Subject Code	COMP6521
Subject Title	Cryptography and Blockchain
Credit Value	3
Level	6
Normal Duration	1 semester
Pre-requisite/ Co-requisite/ Exclusion	Nil
Role and Purposes	To equip students with some basic understanding of cryptography that leads to an understanding of blockchain and cybersecurity. Core cryptographic tools like encryption, authentication, digital signature and key agreement protocols are used behind daily on-line transactions nowadays. Such tools will be covered in the first part of the course. In the second part, students will learn the blockchain mechanism and its various business applications. At the final part of the course, students will be exposed to the threats to the Internet infrastructure. This subject will contribute to the achievement of the DFintech program outcomes by • allowing students to acquire the ability to conduct original applied research in tech-related business areas. (Outcome 3)
Subject Learning Outcomes	Upon completion of the subject, students will be able to: a. use major cryptographic primitives and consider security issues in implementing integrated security functions; b. discuss the inner workings of a typical blockchain-based cryptocurrency; c. leverage smart contracts for various business applications; d. take into account security issues in the TCP/IP protocol suite that can affect the operations of blockchain-based systems; e. adapt existing solutions in the face of emergent security issues.
Subject Synopsis/ Indicative Syllabus	Topic 1. Cryptographic functions and services • Symmetric encryptions, hash functions, message authentication codes, public-key encryption, digital signatures and authentication protocols. Topic 2. Overview of cybersecurity • Types of attacks, threat models and the role of cryptography in network security. Topic 3. Internet security • Link layer security, network layer security, transport layer security and application layer security.

<table>
<tr><td></td><td>Topic 4. Understanding blockchain for cryptocurrencies
• Discover the building blocks of the technology and the operation of blockchain.
• Explore how blockchain plays a central role in cryptocurrencies, and the scope of the blockchain industry.

Topic 5. Blockchain-based applications
• Discover how smart contracts and decentralized applications enable new mechanisms for trading, settlement, clearing, and new forms of business management and organization.
• Investigate key strategic challenges and opportunities in these areas.

Topic 6. Latest trends and concerns
• Explore attacks on blockchain-based systems, and alternatives to traditional blockchains.
• Reflect on how blockchain could change the ways of doing business, and impact industries, consumers and society.</td></tr>
<tr><td>Teaching/Learning Methodology</td><td>The course will be offered in a mode that combines seminars, case studies, team presentations and group discussions.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes
(Note 4)</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="6">Intended subject learning outcomes to be assessed</td></tr>
<tr><td>a.</td><td>b.</td><td>c.</td><td>d.</td><td>e.</td><td></td></tr>
<tr><td>Continuous Assessment*</td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1. Class participation</td><td>20%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>2. Group Case study & presentation</td><td>20%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>3. Individual Assignment</td><td>20%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>4. Individual Assessment (e.g. Test)</td><td>40%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>Total</td><td>100%</td><td colspan="6"></td></tr>
</table>
*Weighting of assessment methods/tasks in continuous assessment may be different, subject to each subject lecturer.

To pass this subject, students are required to obtain Grade D or above in the Continuous Assessment components.

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:</td></tr>
</table>

	1. Class participation aims to stimulate students to critically think, expose and discuss their ideas about concepts, technologies and security issues. 2. The group case study enables students to work as a team to discuss and analyze technical academic proposals. 3. The short written individual assignment in the form of review essay will be used to assess individual student's understanding of the latest cryptography and blockchain technologies and student's critical thinking and analysis of any new applications of technologies. 4. The individual assessment is used to assess individual students' ability to have an overall understanding of the inter-relationship of the various technologies and their individual characteristics.	
Student Study Effort Expected	Class contact:	
	▪ Lectures	30 Hrs.
	Other student study effort:	
	▪ Preparation for the class	30 Hrs.
	▪ Preparation for Assignments	60 Hrs.
	Total student study effort	120 Hrs.
Reading List and References	N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley 2010. R. Anderson, Security Engineering, Second Edition, Wiley 2008. William Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons Inc 2016. Daniel Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, aPress 2017.	