Subject Description Form

Subject Code	COMP5567
Subject Title	Distributed Algorithms and Protocols for Blockchains
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	The objectives of this subject are to: • introduce the principles, concepts, theories, and analysis of distributed algorithms for blockchain systems; • enable the students to analyze the underlying distributed consensus protocols of popular blockchain platforms; and • enable the students to develop basic distributed consensus protocols for blockchain
Intended Learning Outcomes *(Note 1)*	Upon completion of the subject, students will be able to: a) demonstrate a comprehensive understanding of distributed consensus algorithms, including the algorithm design, correctness proof, and complexity analysis; b) possess the ability to analyze the distributed consensus protocols in existing popular blockchain platforms, including Bitcoin, Ethereum, and Hyperledger Fabric; and c) possess the ability of developing basic distributed consensus protocols for blockchains using remote procedure call tools; and d) understand the advanced blockchain consensus protocols with high throughput and high scalability.
Subject Synopsis/ Indicative Syllabus *(Note 2)*	**Introduction to Blockchain Consensus** Architecture of a typical blockchain systems; basics of blockchain consensus; history of consensus protocols; history of blockchain consensus; relationship between traditional consensus and blockchain consensus. **Distributed Consensus Algorithms** System model and problem definition; properties; termination; agreement; integrity; faulty models; Byzantine general problem;

	interactive consistency; impossibility results; synchronous algorithms; correctness analysis; complexity analysis; case studies. **Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance** Hash puzzles; difficulties; forking problem; classic proof of work; ghost protocol; analysis of proof of work protocols; classic proof of stake; centralization issue; improvement proposal; impossibility of byzantine fault tolerance; practical byzantine fault tolerance; comparison and demonstration. **Bitcoin, Ethereum, and Public Blockchains** Architecture of a Bitcoin node; architecture of an Ethereum node; bootstrapping; mining pool; selfish mining; analysis of Bitcoin source code; analysis of Ethereum source code. **Hyperledger Fabric and Federated Blockchains** Architecture of Hyperledger Fabric; peers; endorsers; orderer; ordering services; Kafka; zookeeper; practical byzantine fault tolerance; analysis of Hyperledger Fabric source code. **High Performance Blockchain Consensus** Throughput and scalability; limitations of traditional consensus protocols; hybrid consensus; Bitcoin-NG; parallelization; sharding; trusted execution environments; DAG consensus. **Development of Blockchain Consensus Protocols** Remote procedure calls; remote method invocation; protobuf; gRPC; JSON-RPC; bootstrapping nodes; peer-to-peer network; protocol implementation; case studies.
Teaching/Learning Methodology *(Note 3)*	39 hours of class activities including lectures, tutorials, and labs. • The lectures will be used to deliver course materials; • The tutorials will be used to show case studies to consolidate the understanding of course materials; • The labs will be used to give hands-on guidance to practice exercises.

<table>
<tr><td><b>Assessment Methods in Alignment with Intended Learning Outcomes</b>
<i>(Note 4)</i></td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="4">Intended subject learning outcomes to be assessed</td></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td></tr>
<tr><td>1. Quizzes, assignments, and a project</td><td>60%</td><td>√</td><td>√</td><td>√</td><td>√</td></tr>
<tr><td>2. Exam</td><td>40%</td><td>√</td><td>√</td><td></td><td>√</td></tr>
<tr><td>Total</td><td>100 %</td><td colspan="4"></td></tr>
</table>
<p>Quizzes, assignments and exam will assess students’ understanding of distributed consensus algorithms (a), blockchain consensus protocols (b), and high-performance blockchain consensus protocols (d).</p>
<p>The project will be group basis (1-3 members per group) to assess students’ senses of teamwork and abilities of implementing and developing distributed consensus protocols (c). Each group needs a single submission containing the necessary documents, source codes, etc. as requested, as well as the percentages of contributions for each member (signed by all the members). It is required that each student should contribute at least 30% to the group project. If a student contributes less than 30% to the group project, he/she will receive a ZERO grade; otherwise, the same grade will be assigned to all members of the group.</p>
</td></tr>
<tr><td><b>Student Study Effort Expected</b></td><td>
<table>
<tr><td>Class contact:</td><td></td></tr>
<tr><td>• Class activities (lectures, tutorials, and labs)</td><td>39 Hrs.</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>• Assignments, Quizzes, Projects, Exams</td><td>66 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>105 Hrs.</td></tr>
</table>
</td></tr>
<tr><td><b>Reading List and References</b></td><td>
<p>Books</p>
<p>Lynch, N. A. (1996). Distributed algorithms. Elsevier.</p>
<p>Bashir, I., 2020. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more. Packt Publishing Ltd.</p>
<p>Conference Proceedings and Journals:</p>
<p>ACM SIGSAC Conference on Computer and Communications Security (CCS)</p>
<p>ACM International Conference on Management of Data (SIGMOD)</p>
</td></tr>
</table>

	IEEE Conference on Computer Communications (INFOCOM) IEEE Transactions on Computers IEEE Transactions on Parallel and Distributed Systems Online Materials: https://github.com/bitcoin/bitcoin https://github.com/ethereum/go-ethereum https://github.com/hyperledger/fabric

Note 1: Intended Learning Outcomes
Intended learning outcomes should state what students should be able to do or attain upon subject completion. Subject outcomes are expected to contribute to the attainment of the overall programme outcomes.

Note 2: Subject Synopsis/Indicative Syllabus
The syllabus should adequately address the intended learning outcomes. At the same time, overcrowding of the syllabus should be avoided.

Note 3: Teaching/Learning Methodology
This section should include a brief description of the teaching and learning methods to be employed to facilitate learning, and a justification of how the methods are aligned with the intended learning outcomes of the subject.

Note 4: Assessment Method
This section should include the assessment method(s) to be used and its relative weighting, and indicate which of the subject intended learning outcomes that each method is intended to assess. It should also provide a brief explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes.