CSE3222: Blockchain Foundation & Smart Contract

Programme: B.Tech. (CSE)	Year: 3rd	Semester: 6
Course: Program Elective	Credits: 3	Hours: 40

Course Context and Overview (100 words):

Blockchain is an emerging technology which provides solution to various fields. Its primary objective is to support decentralization. This course will start with the basics of consensus mechanism in a distributed system and fundamental of distributed systems such as failure models, synchronous and asynchronous communication. It will also deal with some of the famous results in distributed consensus algorithms such as FLP impossibility result and DLS consensus result. After the discussion of the basics of distributed consensus, the course will have discussion on the basics of Bitcoin. The second part of the course will have a discussion on scalability issues and solutions such as Payment Channel Network. Moreover, the course will also cover programing language Solidity and security issues in Solidity and Bitcoin.

Prerequisites Courses: Computer Programming, Data Structures & Algorithm, Computer Networks, Computer Security

Course Outcomes (COs):

On completion of this course, the students will have the ability to:	
CO1 :	Understand the basic concepts of distributed consensus algorithms
CO2 :	Understand the basic concepts of Bitcoin
CO3 :	Analyze the scalability issues and solutions
CO4 :	Create distributed application using solidity
CO5 :	Apply the security issues of Bitcoin and Solidity Smart Contract

Course Topics:

Contents	**Lecture Hours**	
UNIT – 1: Distributed Consensus 3		
Introduction: Distributed System, Blockchain, Permissioned/Permissionless Blockchain; Failure Model: Crash, Byzantine; Communication: Synchronous, Asynchronous	1	10
Byzantine Generals Problem, Important Results in Distributed Consensus: FLP, DLS	4	

Consensus Mechanisms: PBFT, PAXOS, RAFT	4	
Research Directions	1	
4 **UNIT-2: Bitcoin Basics** 5		
Basic Cryptographic Tools: Hash, Digital Signature	1	7
Proof of Work (PoW) Consensus	2	
Transaction, Block, Data Structure	1	
Security Issues: Selfish Mining Attack, Routing Attack	3	
6 **UNIT–3: Blockchain Scalability Issues and Solutions** 7		
Scalability Issues: Transaction Throughput, Latency	2	9
Payment Channel Network: Basics, HTLC, Routing issues	4	
Sharding	2	
Research Directions	1	
UNIT-4: Solidity & Smart Contract (Ethereum)		
Structure of a Contract, Types	1	6
Units and Globally Available Variables	1	
Expressions and Control Structures	1	
Contracts	3	
Unit 5: Security issues in Solidity Smart Contract (Ethereum)		
Reentrancy, Denial of Service	2	8
Access Control	2	
Arithmetic issues: Integer Overflow and Underflow	2	
Other Security Issues	2	
Total Lectures		40

Textbook references:
Text Book:

Mostly, the course will be covered through research papers. Research papers and other materials will be provided during the course.

Reference books:

1. Narayanan, Arvind, "*et al. Bitcoin and Cryptocurrency Technologies": A Comprehensive Introduction*. Princeton University Press, 2016.
2. Andreas Antonopoulos, "*Mastering Bitcoin": Programming the Open Blockchain*, 2nd Edition, 2017

Additional Resources:

- Solidity - https://solidity.readthedocs.io/en/v0.7.3/
- Ethereum- http://www.ethdocs.org/en/latest/
- Lightening Network-http://lightning.network/docs/
- Lightening Network- https://lists.linuxfoundation.org/pipermail/lightning-dev/

Evaluation Methods:

Component	**Weightage (%)**
Assignment/Quiz	10%
Project: DApp using solidity in Ethereum/Research Paper Critical Comment and Review	30%
Midterm	20%
Endterm	40%

* **Project:** A team can have a maximum of four members. The team will choose Application or *Research Paper* from the list provided by the instructor or selected by the team with the approval of the instructor. Every team has to submit a report which will consist of Introduction, Literature Review, Code/Critical comment and Conclusion/ Future Work. Each team member will be evaluated individually based on Viva/Presentation/Report/Discussion.

*** Mark Distribution for Project:**
a) Regular Evaluation: 10%
b) Final-Presentation: 10 %
c) Project Report: 10%

Prepared by: Mohit Gupta
Last Update: 20/Oct/2020