SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech II (Semester IV)

Subject Name: Foundations of Blockchain Technology **Subject Code:** BTEA19426
Type of course: Honors (Group: Blockchain Technology)
Prerequisite (if any): Information Security, Cryptography, Networking

Rationale: Blockchain is one of the emerging technologies in today's world. It is a decentralized, distributed ledger that records the provenance of a digital asset. With its inherent design, the data stored via Blockchain would be fully secure in terms of integrity. This course includes the fundamentals behind Blockchain architecture, Block structure, basic cryptographic primitives used to implement Blockchain, the popular crypto-currencies i.e. Bitcoin, Ethereum and the use-cases of Blockchain system.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests) CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No.	Contents	Total Hrs.
1.	**Introduction to Blockchain:** What is Blockchain?, Centralized vs. Decentralized Systems, Centralized Systems, Decentralized Systems, Layers of Blockchain, Application Layer, Execution Layer, Semantic Layer, Propagation Layer, Consensus Layer, Why is Blockchain Important?, Limitations of Centralized Systems, Blockchain Uses and Use Cases	06
2.	**Cryptography and Technical Foundations:** Laying the Blockchain Foundation, Cryptography - Introduction, Mathematics, Confidentiality, Integrity, Authentication, Symmetric Key Cryptography, Asymmetric Key Cryptography, Cryptographic Hash Functions, Hash Algorithms, Merkle trees, Patricia trees, Distributed hash tables (DHTs), Digital signatures, MAC and HMAC, Diffie-Hellman Key Exchange, Symmetric vs. Asymmetric Key Cryptography	10

3.	**Working of Blockchain:** Game Theory, Nash Equilibrium, Prisoner's Dilemma, Byzantine Generals' Problem, Block Chain structure, Blockchain with Merkle Trees, Properties of Blockchain Solutions, Blockchain Transactions, Distributed Consensus Mechanisms, Types of Blockchain-Public, Consortium, Private, Blockchain Implementations - BitCoin, NameCoin, Ripple, Ethereum, Blockchain Collaborative Implementations- Hyperledger, Corda	09
4.	**Bitcoin Blockchain:** The History of Money, Dawn of Bitcoin, What Is Bitcoin?, The Bitcoin Blockchain, Block Structure, The Genesis Block, The Bitcoin Network, Bitcoin Transactions, Consensus and Block Mining, Script Language	08
5.	**Ethereum Blockchain:** From Bitcoin to Ethereum, Ethereum as a Next-Gen Blockchain, Design Philosophy of Ethereum, Ethereum Blockchain, Ethereum Accounts, Merkle Patricia Tree, Ethereum Transaction and Message Structure, Smart Contracts, Ethereum Virtual Machine and Code Execution	08
6.	**Applications of Blockchain:** Financial Services, Insurance, Government, Supply Chain Management, Healthcare, The Internet of Things (IoT)	04

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
20	20	10	10	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

Sr no	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1	Beginning Blockchain - A Beginner's Guide to	Bikramaditya Singhal,	Apress	2018	

	Building Blockchain Solutions	Gautam Dhameja, Priyansu Sekhar Panda	Publishng ISBN: 978-1-4842-3443-3		
2	Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks	Imran Bashir	Packt Publishing ISBN 978-1-78712-544-5	2017	1st Edition
3	Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions	Joseph J. Bambara Paul R. Allen	McGraw Hill ISBN: 978-1-26-011586-4	2018	1st Edition
4	Blockchain for Dummies	Manav Gupta	John Wiley & Sons, Inc. ISBN: 978-1-119-37123-6	2017	

Course Outcomes:

Sr. No.	CO Statements	Marks % weightage
CO-1	Identify emerging abstract models for Blockchain Technology	20%
CO-2	Explain the fundamental cryptographic technology used to implement Blockchain system	20%
CO-3	Describe the block structure, transactions and working of Blockchain mechanism	20%
CO-4	Describe the basics of the first generation cryptocoin-Bitcoin and its working	15%
CO-5	Differentiate the second generation Blockchain technology- Ethereum from Bitcoin	15%
CO-6	Visualize the application of Blockchain with real-life case studies.	10%

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

List of Open learning website:

1. NPTEL: Introduction to Blockchain Technology and Applications (https://nptel.ac.in/noc/courses/noc20/SEM1/noc20-cs01/)
2. NPTEL: BLOCKCHAIN ARCHITECTURE DESIGN AND USE CASES (https://nptel.ac.in/courses/106/105/106105184/)

List of Open Source Software:

1. OpenSSL
2. Moralis.io

SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

For Lab Sessions:

Practical List

Sr. No	Practical Statements
1.	Study OpenSSL crypto library and various commands.
2.	Install OpenSSL and use various commands to perform the following a) Encrypt and decrypt a message using AES. b) Generate public-private key pairs for RSA. Also encrypt and decrypt a given message using RSA keys. c) Generate public-private key pairs for ECC. Also encrypt and decrypt a given message using ECC keys. d) Generate SHA256 message digest for a given message. e) Generate RSA digital signature, sign a given message and verify the signature. f) Generate ECDSA digital signature.
3.	Write a Java Program to Encrypt/Decrypt a given message using RSA algorithm.
4.	Write a Java Program to Encrypt/Decrypt a given message using AES algorithm (use inbuild class/packages).
5.	Write a Java Program to generate SHA256 message digest.
6.	Write a Java Program to generate digital signature, sign a message and verify the signature.