Programme	**Bachelor of Technology in Computer Science and Engineering**	Academic Year of Regulation	**2018-2019**
Department	**Computer Science and Engineering**	Semester	**VII**

Course Code	Course Name	Credit Structure				Marks Distribution			
		L	T	P	C	INT	MID	END	Total
CS 417	**Blockchain Technologies**	**3**	**0**	**0**	**3**	**50**	**50**	**100**	**200**

Course Objectives	This course explains the need and working principle of blockchain systems, cryptocurrency, cryptographic primitives.	Course Outcomes	CO1	Able to explain the need of Blockchain system and demonstrate the fundamentals of cryptocurrency, cryptographic primitives.
	This course describes the in-depth knowledge and concept of recent technologies, tools, and implementation strategies.		CO2	Able to demonstrate the tools, Nakamoto consensus and demonstrate the working principals of payment verification protocol
	This course provides the validation and verification techniques of transaction through miners and Consensus Algorithms.		CO3	Able to describe and analyse the various consensus algorithm as per the application requirements.
	This course provides the mechanism for the development of smart contract using solidity language for distributed applications.		CO4	Able to design and develop the communication model for sending and receiving the messages in transaction.
			CO5	Able to design, develop and analyse the real time distributed real time applications.

No.	COs	Mapping with Program Outcomes (POs)												Mapping with PSOs		
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
1	CO1	3	3	-	-	-	-	-	-	2	-	-	-	3	-	3
2	CO2	3	3	3	1	2	-	-	-	1	-	-	-	2	3	2
3	CO3	1	2	3	3	2	2	-	-	-	-	-	-	2	3	3
4	CO4	1	2	3	3	3	2	3	-	2	-	-	1	2	3	2
5	CO5	2	3	3	2	2	3	2	-	2	-	-	1	3	3	3

SYLLABUS			
No.	Content	Hours	COs
I	Blockchain Introduction and Overview: Background and evolution of technology, Distributed systems, Distributed Ledger: DLT concept, features, benefits and relevance in application, Security and Privacy: Cryptography, Hash, Permission	03	CO1
II	Cryptographic primitives: Symmetric cryptography, A Symmetric cryptography, DES, Hash functions, Patricia trees, Distributed hash tables (DHTs), Digital signatures, Sign then encrypt, Encrypt then sign Elliptic Curve Digital signature algorithm (ECDSA), How to generate a digital signature, ECDSA using OpenSSL Homomorphic encryption, Signcryption, Zero knowledge proofs, Blind signatures, Encoding schemes	04	CO1
			CO2
III	Bitcoin, Bitcoin definition, Keys and addresses, Public keys in bitcoin, Private keys in bitcoin, Bitcoin currency units, Base58Check encoding, Vanity addresses	04	CO2
IV	Transactions, The transaction life cycle, The transaction structure, The script language, Commonly used Opcodes, Types of transaction, Transaction fee, Contracts, Transaction malleability, Transaction pools	04	CO3
V VI	Blockchain ,The structure of a block, The structure of a block header, The genesis block Mining, Task of miners Synching up with the network,Proof of Work, The mining algorithm, The hashing rate, Mining systems CPU, GPU, FPGA, ASICs, Mining pools	05	CO3
			CO4
VII	The bitcoin network: Wallets, Payments: Bitcoin investment and buying and selling bitcoins,Bitcoin installation, Bitcoin programming and the command-line interface, Bitcoin improvement proposals (BIPs)	04	CO3
			CO4
	Alternative Coins: Theoretical foundations, Alternatives to Proof of Work, Non-outsourceable puzzles Difficulty adjustment and retargeting algorithms, Bitcoin limitations, Extended protocols on top of bitcoin Development of altcoins, Consensus algorithms, Coin, Mining guide, Zcash	05	CO4
VIII	Smart Contracts: Definition, Ricardian contracts, Ethereum 101 Introduction: Ethereum blockchain, Transactions, Contract creation transaction, Message call transaction, Elements of the Ethereum blockchain, Ethereum virtual machine (EVM), Precompiled contracts, Accounts, Blocks, Transaction and Block validation mechanism	04	CO5
IX	Ethereum Development: Tools and Client, Introduction to Solidity, Hyperledger, Protocols, Applications outside the currencies.	03	CO5
	Total	**36**	

Essential Readings

1. Imran Bashir, Mastering Blockchain,1/E,Packt, 2017.

2. Melanie Swan, Blockchain: Blueprint for New Economy, 1/E, O'Reilly Media, 2015.

3. Sam Goundar, Blockchain Technologies, Applications And Cryptocurrencies: Current Practice And Future Trends, 1/E Word Scientific, 2020

Supplementary Readings

1. Alan T. Norman, Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts,1/E, [United States?] : Alan T. Norman,2017

2. Jan Veuger, Blockchain Technology and Applications, 1/E, Nova Publisher,2019

3. Andreas Bolfing, Cryptographic Primitives in Blockchain Technology : A Mathematical Introduction, 1/E, Oxford University Press, 2020.