

<b>Semester: 3</b>	<b>Course No.: 302</b>	<b>Course Code: FTM206-2C</b> <b>Course Title: - Blockchain and Cryptocurrency</b>
<b>Credits: 4</b>	<b>Course Category: MAJOR COURSE</b>	

**Course Outcomes: On successful completion of the course the learner will be able to**

<b>CO#</b>	<b>COGNITIVE ABILITIES</b>	<b>COURSE OUTCOMES</b>
<b>CO1</b>	<b>REMEMBERING</b>	Recall fundamental concepts, terminology, and key figures related to blockchain technology, cryptography, consensus mechanisms, blockchain platforms, cryptocurrencies, and their applications
<b>CO2</b>	<b>UNDERSTANDING</b>	Explain the underlying principles, functionalities, and interrelationships between blockchain technology, cryptographic techniques, consensus algorithms, smart contracts, cryptocurrency mechanisms, and their broader ecosystem.
<b>CO3</b>	<b>APPLYING</b>	Compare and contrast different types of blockchains, consensus mechanisms, cryptocurrency wallets and exchanges, and analyse the basic processes involved in cryptocurrency transactions and smart contract deployment.
<b>CO4</b>	<b>ANALYSING</b>	Evaluate the security and operational trade-offs associated with various blockchain designs, consensus protocols, and cryptocurrency mechanisms, and analyse the potential impact of decentralization on traditional financial systems
<b>CO5</b>	<b>EVALUATING</b>	Assess the suitability of different blockchain platforms and cryptocurrencies particularly within the FinTech domain, considering their advantages, limitations of current trends and regulatory landscapes.

<b>Unit No.</b>	<b>Unit Contents</b>	<b>Sessions Allotted</b>
<b>1</b>	<p><b>Introduction to Blockchain: Core Concepts and Enabling Cryptography</b></p> <ul style="list-style-type: none"> <li>○ Introduction to Blockchain:</li> <li>○ Core Concepts: Definition, Blocks, Chains, Transactions, Hash Pointers, Immutability, Transparency, Distributed Ledger Technology (DLT).</li> <li>○ History &amp; Evolution: Brief overview from Blockchain 1.0 to foundational concepts.</li> <li>○ Types of Blockchain</li> <li>○ Generic Elements: Nodes (Full, Light), Network Topology, Ledger structure, Transaction lifecycle (creation to confirmation).</li> <li>○ Design Primitives Overview: Introduction to the roles of Cryptography, Protocols, Security models, Consensus algorithms, Permissions, and Privacy.</li> <li>○ Basic Crypto Primitives: Hash Functions: Properties, SHA-256, Keccak-256. Role in linking and integrity.</li> <li>○ Digital Signatures: Public Key Cryptography (Asymmetric), ECC basics, ECDSA. Role in authentication and ownership.</li> <li>○ Merkle Trees: Structure, purpose (efficient verification).</li> <li>○ Blockchain Cryptography Techniques: Symmetric vs. Asymmetric Cryptography overview and relevance.</li> <li>○ Privacy &amp; Security Considerations: Anonymity vs. Pseudonymity in public blockchains.</li> <li>○ Multi-Signature (Multi-Sig) Wallets: Concept and basic use cases for security.</li> </ul>	<b>15</b>

2	<p><b>Consensus, Platforms, and Smart Contracts</b></p> <p><b>Consensus Mechanisms:</b></p> <ul style="list-style-type: none"> <li>• Need for Consensus: The problem of agreement, Byzantine Generals Problem (briefly).</li> <li>• Requirements: Safety and Liveness properties, differences in permissionless vs. permissioned.</li> <li>• Detailed Study of: <ul style="list-style-type: none"> <li>○ Proof-of-Work (PoW): Mechanism, Advantages, Disadvantages (Energy, Scalability), Bitcoin's use case.</li> <li>○ Proof-of-Stake (PoS): Mechanism, Variations (briefly), Advantages, Disadvantages (Centralization risks), Ethereum's transition.</li> </ul> </li> <li>• Brief mention of Proof-of-Authority (PoA) and its application in permissioned settings.</li> <li>• Scalability Aspects: Understanding how consensus choices impact throughput and latency (introduction).</li> </ul> <p><b>Blockchain Platforms:</b></p> <ul style="list-style-type: none"> <li>• Public Blockchains: <ul style="list-style-type: none"> <li>○ Introduction to Ethereum: Role as a smart contract platform, Ether (ETH), Gas concept.</li> <li>○ Smart Contracts: Definition, concept of code-as-law, immutability.</li> <li>○ Development: Introduction to Solidity (purpose, basic structure - maybe a very simple example).</li> <li>○ Issues: Correctness and Verifiability challenges, Common vulnerabilities overview.</li> </ul> </li> <li>• Permissioned Blockchains: <ul style="list-style-type: none"> <li>○ Design Goals: Enterprise focus, Privacy, Scalability, Governance.</li> <li>○ Consensus: Overview of protocols suited for permissioned settings (e.g., Raft, IBFT - briefly).</li> <li>○ Introduction to Hyperledger Fabric: Key architecture concepts (Peers, Orderers, Channels - conceptually).</li> </ul> </li> </ul>	15
3	<p><b>Fundamentals and Ecosystem of Cryptocurrencies</b></p> <ul style="list-style-type: none"> <li>• Definition: Digital/virtual currency secured by cryptography.</li> <li>• History: Bitcoin &amp; Ethereum origins, Rise of Altcoins (brief overview of key early projects).</li> <li>• Types: Coins vs. Tokens (Utility, Security, Governance) - clear distinctions and examples.</li> <li>• Wallets: Types (Software, Hardware, Paper, Hot vs. Cold), Public/Private Keys</li> <li>• Exchanges: Centralized (CEX) vs. Decentralized (DEX) - how they work, pros/cons from a user and market perspective.</li> <li>• Transaction Processing: How cryptocurrency transactions are created, signed, broadcast, and confirmed on the blockchain (Miner/Validator role with crypto focus).</li> <li>• Mining &amp; Staking: Deeper look at the incentive mechanisms behind PoW and PoS in the context of earning cryptocurrencies. Mining Pools and their impact.</li> <li>• Brief overview of factors influencing cryptocurrency prices (Supply/Demand, Adoption, Regulation, Market Sentiment, News).</li> </ul>	15
4	<p><b>Applications, Trends, and Risks of Cryptocurrencies</b></p> <p><b>FinTech &amp; Decentralized Finance (DeFi):</b></p> <ul style="list-style-type: none"> <li>• Decentralized Finance (DeFi): Core concepts (Composability, Openness) with a focus on cryptocurrency use cases.</li> </ul>	15

	<ul style="list-style-type: none"> <li>• Key DeFi Applications: Lending/Borrowing platforms (Aave, Compound) and their reliance on cryptocurrencies, Decentralized Exchanges (Uniswap) for trading cryptocurrencies, Yield Farming and its incentives.</li> <li>• Other FinTech Uses: Cross-border Payments/Remittances using cryptocurrencies, Tokenization of assets (briefly).</li> </ul> <p><b>Digital Assets &amp; DAO:</b></p> <ul style="list-style-type: none"> <li>• Non-Fungible Tokens (NFTs): Concept, use cases related to digital ownership and cryptocurrency interaction (marketplaces, buying/selling).</li> <li>• Decentralized Autonomous Organizations (DAOs): Concept, structure, governance models with examples of cryptocurrency-driven DAOs.</li> </ul> <p><b>Risks &amp; Issues:</b></p> <ul style="list-style-type: none"> <li>• Volatility: Understanding the high price fluctuations in cryptocurrency markets.</li> <li>• Security Risks: Hacks of exchanges and wallets, scams, phishing targeting cryptocurrency holders.</li> <li>• Regulatory Uncertainty: Global landscape of cryptocurrency regulation and its impact.</li> <li>• Sustainability Concerns (PoW's impact on specific cryptocurrencies).</li> <li>• Future Trends in Cryptocurrencies: Scalability solutions (Layer-2 focused on crypto transactions), Interoperability between different cryptocurrencies.</li> </ul>	
--	--	--

**Suggested Text Books:**

1. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher
2. "Mastering Bitcoin: Programming the Open Blockchain" by Andreas M. Antonopoulos (2nd Edition, 2017)
3. "The Bitcoin Standard: The Decentralized Alternative to Central Banking" by Saifedean Ammous (2018)

**Suggested Reference Books:**

- "Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond" by Chris Burniske and Jack Tatar (2017)