Subject: Elective 1 : Blockchain Technology and Security			
Program: M.Sc. in CyberSecurity		Subject Code:	Semester: II

Teaching Scheme				Examination Evaluation Scheme				
Lecture	Tutorial	Practical	Credits	University Theory Examination	University Practical Examination	Continuous Internal Evaluation (CIE)-Theory	Continuous Internal Evaluation (CIE)-Practical	Total
2	0	2	3	40	40	60	60	200

COURSE OBJECTIVES:

1. Provide a foundational understanding of blockchain concepts, including decentralization, consensus mechanisms, and various blockchain types.

2. Explore the architecture and components of blockchain systems, covering topics such as block structure, cryptographic functions, and smart contracts.

3. Address fundamental security principles in blockchain, focusing on cryptographic techniques, key management, and best practices to mitigate threats.

4. Advance participants' knowledge by examining privacy, permissioned blockchains, security auditing, regulatory compliance, and emerging trends in blockchain security.

Content

Course Content		W - Weightage (%) , T - Teaching hours		
Sr.	**Topics**		**W**	**T**
1	**Introduction to Blockchain Technology** ● **Definition and Basics of Blockchain** ● **Historical Evolution of Blockchain** ● **Key Concepts: Decentralization, Consensus Mechanisms, Immutability** ● **Types of Blockchains: Public, Private, Consortium** ● **Use Cases and Applications**		20	10
2	**Blockchain Architecture and Components** ● **Structure of a Block** ● **Cryptographic Hash Functions** ● **Merkle Trees** ● **Blockchain Nodes: Miners, Validators, Full Nodes** ● **Smart Contracts and DApps** ● **Forks and Consensus Algorithms (e.g., Proof of Work, Proof of Stake)**		20	10

3	**Blockchain Security Fundamentals**	20	10
	• **Security Challenges in Traditional Systems** • **Blockchain Security Features** • **Cryptographic Techniques in Blockchain** • **Secure Key Management** • **Security Best Practices for Smart Contracts** • **Threats and Attacks on Blockchain Networks**		
4	**Advanced Blockchain Security**	20	9
	• **Privacy and Anonymity in Blockchain** • **Permissioned Blockchains and Access Control** • **Security Auditing and Testing** • **Regulatory Compliance in Blockchain** • **Case Studies: Notable Security Incidents and Lessons Learned** • **Future Trends and Innovations in Blockchain Security**		

1. TEXTBOOKS and REFERENCE BOOKS:

1. "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" by Andreas M. Antonopoulos

2. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher

3. "Blockchain Applications: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti

4. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" by Imran Bashir

5. "Blockchain Security: A Comprehensive Guide to Safe Cryptocurrency Transactions" by Merkle Bloom LLC

List of Practicals:

List of Practical	
1.	Hands-on session explaining the structure of a blockchain.
2.	Group activity to identify and analyze potential blockchain use cases.
3.	Practical exercise on understanding the structure of a block.
4.	Introduction to basic smart contract development.
5.	Participants explore and configure security settings on a blockchain network.

6.	Group activity to identify potential threats to a blockchain network.
7.	Practical session on privacy and anonymity features in a blockchain.
8.	Hands-on security auditing exercises on smart contracts.
9.	Case study analysis of regulatory compliance challenge
10.	Practical activity where participants set up and interact with a blockchain network.