**Lesson Plan**

**B.E. (ECS) (Semester VII)**

 **Subject: BLOCK CHAIN TECHNOLOGIES**

**Subject code: ECCDO702**

**Teacher-in-charge: Prof.Prajakta Bhangale**

**Academic Term: July – October 2022**

| **ModuleNo.** | **Contents** | **Hrs.** |
| --- | --- | --- |
| **1** | **Introduction of Cryptography** | **04** |
| Basic Cryptographic primitives used in Blockchain - Public Key cryptosystem,Cryptographic Hash functions: Properties of Hash, MD5, SHA 256, Hash Pointersand Data Structures, Digital Signatures: ECDSA, Public Keys as Identities,Cryptocurrencies: Goofycoin |
| **2** | **Introduction to Blockchain** | **07** |
| Centralization vs. Decentralization, What is Blockchain, History of Blockchain,Blockchain defined- peer to peer, Distributed Ledger, Cryptographically Secure,Append-only, Updatable via consensus, How Blockchain Works, Benefits andLimitations of Blockchain, Types of Blockchain, The Structure of a Block, Blockheader, Genesis block, Mining , Rewards, Consensus, Types of ConsensusMechanisms, Consensus in Blockchain. |
|
|
|
| **3** | **Bitcoin and Cryptocurrency** 6 | **06** |
| What is Bitcoin, Private keys in Bitcoin, Public Keys in Bitcoin, Addresses inBitcoin, Transactions, The Bitcoin Network,Bitcoin Wallets, Scripting language inBitcoin, Bitcoin Mining- task of Bitcoin miners, Mining Hardware, CryptoCurrencies, Anonymity and Pseudonymity in BitcoinSelf Study - Alt Coins |
| **4** | **Introduction to Ethereum** | **10** |
| Introduction to Ethereum, Ethereum’s Consensus Mechanisms, MetaMask Setup,Ethereum Accounts, Ethers, Gas, Introduction to Smart Contracts, Remix IDE,Writing smart contracts using SoliditySelf Study- Geth, Ganache-Creating Wallets |
| **5** | **Introduction to Hyperledger** | **06** |
| What is Hyperledger? Distributed Ledger Technology & its Challenges, Hyperledger& Distributed Ledger Technology, Hyperledger Fabric, Hyperledger Composer,Transaction Flow.Self study: Case Study of Supply Chain Management using Hyperledger |
| **6** | **Privacy, Security issues in Blockchain** | **10** |
| Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymitypreservation, attacks on Blockchains (Sybil attacks, selfish mining, 51% attacks),prevention of attacksSelf Study: Corda, Ripple, Quorum platforms and its security |
| **Total** | **39** |

**Course Objectives:**

1. To learn the fundamentals of Blockchain

2. To obtain knowledge about technologies of Blockchain

3. To incorporate the models of Blockchain- Ethereum

4. To learn the models of Hyperledger Fabric

5. To explore various applications of Blockchain.

**Course Outcomes:**

**After successful completion of the course students will be able to:**

1. Describe the primitives of the cryptography related to blockchain.

2. Understand and explore the working of Blockchain technology

3. Illustrate the concepts of Bitcoin and their usage.

4. Implement Ethereum block chain contract.

5. Explore Hyperledger Fabric and its working.

6. Investigate security features in blockchain technologies

**CO-PO-PSO Mapping:**

|  | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO 11** | **PO 12** | **PSO1** | **PSO2** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ECCDO702.1** | 3 | 2 |  |  |  |  |  |  |  |  |  |  |  |  |
| **ECCDO702.2** | 3 |  |  |  |  |  |  |  | 2 | 2 |  |  |  |  |
| **ECCDO702.3** | 3 | 2 |  |  |  |  |  |  | 2 | 2 |  |  |  |  |
| **ECCDO702.4** | 3 | 2 |  |  | 2 |  |  |  | 2 |  |  |  |  |  |
| **ECCDO702.5** | 3 | 2 |  |  |  |  |  |  | 2 |  |  |  |  |  |
| **ECCDO702.6** | 3 | 2 |  |  |  |  |  |  | 2 |  |  |  |  |  |

**Provide justification of PO to CO mapping**

| **ECCDO702.1** | **PO1** | 1.1.1 Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems 1.1.2 Apply the concepts of probability, statistics and queuing theory in modeling of computer-based system, data and network protocols.1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| --- | --- | --- |
| **PO2** | 2.1.3 Identify processes/modules/algorithms of a computer-based system and parameters to solve the problems2.1.4 Identify mathematical algorithmic knowledge that applies to a given problem |
| **ECCDO702.2** | **PO1** | 1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| **PO9** | (Presentations on various topics)9.1.1 Recognize a variety of working and learning preferences; appreciate the value of diversity on a team 9.1.2 Implement the norms of practice (e.g. rules, roles, charters, agendas, etc.) of effective team work, to accomplish a goal.9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations |
|  | **PO10** | 10.2.1 Listen to and comprehend information, instructions, and viewpoints of others 10.2.2 Deliver effective oral presentations to technical and non-technical audiences |
| **ECCDO702.3** | **PO1** | 1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| **PO2** | 2.1.3 Identify processes/modules/algorithms of a computer-based system and parameters to solve the problems2.1.4 Identify mathematical algorithmic knowledge that applies to a given problem |
| **PO9** | (Presentations on various topics)9.1.1 Recognize a variety of working and learning preferences; appreciate the value of diversity on a team 9.1.2 Implement the norms of practice (e.g. rules, roles, charters, agendas, etc.) of effective team work, to accomplish a goal.9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations |
|  | **PO10** | 10.2.1 Listen to and comprehend information, instructions, and viewpoints of others 10.2.2 Deliver effective oral presentations to technical and non-technical audiences |
| **ECCDO702.4** | **PO1** | 1.1.1 Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems 1.1.2 Apply the concepts of probability, statistics and queuing theory in modeling of computer-based system, data and network protocols.1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| **PO2** | 2.1.3 Identify processes/modules/algorithms of a computer-based system and parameters to solve the problems2.1.4 Identify mathematical algorithmic knowledge that applies to a given problem |
| **PO5** | 5.1.1 Identify modern engineering tools, techniques and resources for engineeringactivities  |
|  | **PO9** | (Presentations on various topics)9.1.1 Recognize a variety of working and learning preferences; appreciate the value of diversity on a team 9.1.2 Implement the norms of practice (e.g. rules, roles, charters, agendas, etc.) of effective team work, to accomplish a goal.9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations |
| **ECCDO702.5** | **PO1** | 1.1.1 Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems 1.1.2 Apply the concepts of probability, statistics and queuing theory in modeling of computer-based system, data and network protocols.1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| **PO2** | 2.1.3 Identify processes/modules/algorithms of a computer-based system and parameters to solve the problems2.1.4 Identify mathematical algorithmic knowledge that applies to a given problem |
| **PO5** | 5.1.1 Identify modern engineering tools, techniques and resources for engineeringactivities  |
| **ECCDO702.6** | **PO1** | 1.1.1 Apply the knowledge of discrete structures, linear algebra, statistics and numerical techniques to solve problems 1.1.2 Apply the concepts of probability, statistics and queuing theory in modeling of computer-based system, data and network protocols.1.3.1 Apply engineering fundamentals1.4.1 Apply theory and principles of Electronics and/or computer science and engineering to solve an engineering problem |
| **PO2** | 2.1.3 Identify processes/modules/algorithms of a computer-based system and parameters to solve the problems2.1.4 Identify mathematical algorithmic knowledge that applies to a given problem |
| **PO9** | (Presentations on various topics)9.1.1 Recognize a variety of working and learning preferences; appreciate the value of diversity on a team 9.1.2 Implement the norms of practice (e.g. rules, roles, charters, agendas, etc.) of effective team work, to accomplish a goal.9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations9.2.1 Demonstrate effective communication, problem-solving, conflict resolution and leadership skills 9.2.2 Treat other team members respectfully 9.2.3 Listen to other members 9.2.4 Maintain composure in difficult situations |

**CO Assessment Tools:**

| ***Course Outcome*** | ***direct Method (80%)*** | ***Indirect Method (20%)*** |
| --- | --- | --- |
| Unit Tests | Presentations | End Sem Exam | Course exit survey |
| 1 | 2 |
| **ECCDO702.1** | 40% | -- | 30% | 30% | 100% |
| **ECCDO702.2** | 40% | -- | 30% | 30% | 100% |
| **ECCDO702.3** | 40% | --- | 30% | 30% | 100% |
| **ECCDO702.4** | -- | 40% | 30% | 30% | 100% |
| **ECCDO702.5** |  | 40% | 30% | 30% | 100% |
| **ECCDO702.6** |  | 40% | 30% | 30% | 100% |

**CO calculation= (0.8 \*Direct method + 0.2\*Indirect method)**

**Curriculum Gap identified: (with action plan)**

Blockchain needs basic prerequisite of Mathematical concepts which are not there in the syllabus **.**

**Action:** Lecture for explaining concepts about Modulus functions for Security is conducted.

Content beyond syllabus:NIL

**Modes of content delivery**

| **Modes of Delivery** | **Brief description of content delivered** |
| --- | --- |
| Class room lecture |  PPTS,Whiteboard |
| Presentations | PPTS  |

**Text Books:**

* Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, 2016.
* Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.

**Reference Books:**

* Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018
* D. Drescher, Blockchain Basics. Apress, 2017.
* Merunas Grinčelaitis, “Mastering Ethereum: Implement Advanced Blockchain Applications Using Ethereum-supported Tools, Services, and Protocols”, Packt Publishing.
* Blockchain with Hyperledger Fabric,Luc Desrosiers, Nitin Gaur, Salman A. Baset, Venkatraman Ramakrishna, Packt Publishing.

 ***Lesson Plan***

| **CLASS** | **BE Electronics and Computer Science, Semester VII** |
| --- | --- |
| Academic Term  | July- October 2022 |
| Subject | **Blockchain Technology(ECCDO702)** |
| ***Periods (Hours) per week*** | ***Lecture*** | ***3*** |
| ***Practical*** | ***NIL*** |
| ***Tutorial*** | ***NIL*** |
| ***Evaluation System*** |  | ***Hours*** | ***Marks*** |
| Theory examination | 3 | 80 |
| Internal Assessment | -- | 20 |
| Practical Examination | -- | -- |
| Oral Examination | -- | -- |
| Term work | -- | -- |
| Total | -- | 100 |
|  |
| ***Time Table*** | ***Day*** | ***Time*** |
| Wednesday | 12-1 |
| Thursday  | 2.30-3.30 |
| Friday  | 12-1 |
| ***Course Content and Lesson plan*** |
| **Week** | **Lecture** **No.** | **Date** | **Topic** |  |
| **Planned** | **Actual** |  | **Remarks****(If any)** |
| ***Module 1:*  Introduction of Cryptography** |
| 1 | 1 | 18/7 | 18/7 | Basic Cryptographic primitives used Blockchain - Public Key cryptosystem, |  |
| 2 | 19/7 | 19/7 | Cryptographic Hash functions: Properties of Hash, MD5 |  |
| 3 | 20/7 | 23/7 | SHA 256,Digital signature | Lecture adjusted on Saturday |
| 4 | 25/7 | 25/7 | Hash Pointers, ECDSA, Public Keys as Identities,Cryptocurrencies: Goofycoin and Data Structures, |  |
|  | **Module2: Introduction to Blockchain** |
| 2 | 5 | 26/7 | 26/7 | Centralization vs. Decentralization, What is Blockchain, History of Blockchain |  |
| 6 | 27/7 | 27/7 | Blockchain defined- peer to peer, Distributed Ledger |  |
| 7 | 3/8 | 3/8 | Cryptographically Secure,Append-only, Updatable via consensus,  |  |
| 8 | 4/8 | 4/8 | How Blockchain Works, Benefits andLimitations of Blockchain, |  |
| 9 | 5/8 | 5/8 | Types of Blockchain, The Structure of a Block, Block header, Genesis block, |  |
| 10 | 10/8 | 10/8 | Mining , Rewards, |  |
| 11 | 11/8 | 11/8 | Consensus, Types of ConsensusMechanisms, Consensus in Blockchain. |  |
| **Module 3: Bitcoin and Cryptocurrency** |
| 3 | 12 | 12/8 | 12/8 | What is Bitcoin, Private keys in Bitcoin, Public Keys in Bitcoin |  |
| 13 | 17/8 | 17/8 | Addresses in Bitcoin, Transactions, The Bitcoin Network,Bitcoin Wallets,  |  |
| 14 | 18/8 | 18/8 | Scripting language in Bitcoin |  |
| 15 | 19/8 | 18/8 | Bitcoin Mining- task of Bitcoin miners, Mining Hardware, |  |
| 16 | 24/8 | 19/8 | Crypto Currencies, |  |
| 17 | 25/8 | 24/8 | Anonymity and Pseudonymity in Bitcoin |  |
| **Module 4: Introduction to Ethereum** |
| 4 | 18 | 26/8 | 25/8 | Introduction to Ethereum, Ethereum’s Consensus Mechanisms, |  |
| 19 | 8/9 | 26/8 | MetaMask Setup,Ethereum Accounts, Ethers, Gas |  |
| 20 | 9/9 | 8/9 | MetaMask Setup, |  |
| 21 | 14/9 | 9/9 | MetaMask Setup |  |
| 22 | 15/9 | 21/9 | Ethereum Accounts, Ethers, Gas |  |
| 23 | 16/9 | 22/9 |  Introduction to Smart Contracts, |  |
| 24 | 21/9 | 23/9 | Writing smart contracts using Solidity |  |
| 25 | 22/9 | 28/9 | Remix IDE |  |
| **Module 5: Introduction to Hyperledger** |
| 5 | 26 |  23/9 | 29/9 | What is Hyperledger? Distributed Ledger Technology & its Challenges |  |
| 27 |  28/9 | 6/10 | Hyperledger & Distributed Ledger Technology |  |
| 28 |  29/9 | 7/10 | Hyperledger Fabric |  |
| 29 |  30/9 | 13/10 |  Hyperledger Composer, |  |
| 30 | 6/10 | 14/10 | Transaction Flow. |  |
| 6 | **Module 6: Privacy, Security issues in Blockchain**6/10 |
| 31 | 7/10 | 20/10 | Pseudo-anonymity vs. anonymity, |  |
| 32 | 13/10 | 20/10 | Zcash and Zk-SNARKS for anonymitypreservation, |  |
| 33 | 14/10 | 21/10 |  attacks on Blockchains (Sybil attacks, selfish , Prevention of attacks mining, 51% attacks), |  |
|  | 34 | 20/10 | 22/10 | Presenatation(online) 3hrs |  |
| ***Total*** | 34 |  |  |  |  |

**Examination Scheme**

| Module | Lecture Hours | Marks distribution in Test (For internal assessment/TW) | Approximate Marks distribution in Sem. End Examination |
| --- | --- | --- | --- |
| Test 1 | Test 2 |
| 1 | Introduction To cryptography | 04 | 5 |  |  |
| 2 | Introduction To Blockchain  | 07 | 10 |  |  |
| 3 | Bitcoin and cryptocurrency  | 06 | 5 |  |  |
| 4 | Introduction to Ethereum | 10 |  | 5 |  |
| 5 | Introduction to Hyperledger | 06 |  | 5 |  |
| 6 | Privacy, Security issues in Blockchain  | 10 |  | 10 |  |

**Identification of Strong and Weak Students using Test**

|  |  | **No of Students** |
| --- | --- | --- |
| **Test No.** | **Test Date** | **Total Students** | **Full Marks** | **>80%**  | **79%>marks>60%** | **less than 60%** | **Failed** |
| **1** | **16/9** | **23** | **0** | **0** | **6** | **17** | **1** |
| **2** | **18/10** | **23** | **0** | **3** | **13** | **7** | **1** |

| **Classification: Tool (Test)** | **Category** |
| --- | --- |
| Strong students | Students scoring above 60% |
| Weak Students | Students scoring below 50% |

| **Submitted By**  | **Approved By** |
| --- | --- |
| Prof.Prajakta Bhangale | ii) Dr. D. V. Bhoir Sign: |
| Sign: | ii) Prof. K. Narayanan Sign: |
|   | iii) Prof. Shilpa Patil Sign: |
|  |  |
|  |  |
| **Date of Submission:** | **Date of Approval:** |
|  |
| **Remarks by PAC (if any)** |
|  |
|  |