

GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)**Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)**

Semester -VI

Course Title: **Foundation of Block chain**

(Course Code: 4361603)

Diploma programme in which this course is offered	Semester in which offered
Information Technology	Sixth

1. RATIONALE:

Application of Blockchain is vast in nature and is adapted in industries including finance, healthcare, supply chain management, and real estate. Foundation of Blockchain course introduces principles of cryptography and basic concepts of cryptography and applies in Blockchain and distributed ledger technology. Understanding the concept of cryptography will help to move smoothly to the fundamentals of the Blockchain and distributed ledger systems. This course focuses on the building blocks of Blockchain: Blockchain data structure, Blockchain types, block rewards, Consensus mechanisms and distributed ledger and user identification. These concepts help understand conceptualization of Blockchain in the application of cryptocurrency.

2. COMPETENCY:

The purpose of this course is to help the student to attain the following industry identified competency through various teaching learning experiences:

- ☐ Understand the Blockchain and its building blocks to develop a distributed ledger system and cryptocurrency.

3. COURSE OUTCOMES (COs):

The practical exercises, the underpinning knowledge and the relevant soft skills associated with this competency are to be developed in the student to display the following COs:

- a) Understand concepts of cryptography, Blockchain and distributed ledger.
- b) Categorize Blockchain structure and Blockchain types.
- c) Examine Consensus mechanism and attack types in Blockchain.
- d) Apply concepts of cryptography and Blockchain in cryptocurrency.
- e) Understand decentralization with the help of Blockchain.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T/2+P/2)	Examination Scheme				
L	T	P	C	Theory Marks		Practical Marks		Total Marks
				CA	ESE	CA	ESE	

3	0	4	5	30	70	25	25	150
---	---	---	---	----	----	----	----	-----

(*): Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

Legends: **L**-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** -Practical; **C** – Credit, **CA** - Continuous Assessment; **ESE** -End Semester Examination.

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) are the sub-components of the COs. These PrOs need to be attained to achieve the COs.

Sr. No.	Practical Outcome (PrOs)	Unit No.	Approx. Hrs. required
1	Implement following concept to get understanding of applications of cryptography in Blockchain foundation. 1.1 Diffie-Hellman Key exchange algorithm. 1.2 RSA algorithm. 1.3 SHA1 Hashing algorithm.	I	12
2	Implement following concept to understand the Blockchain and its implementation. 2.1 Creating a Merkle tree. 2.2 Creation of a block for Blockchain. 2.3 Block chain Implementation Programming code. 2.4 Creating ERC20 token. 2.5 Java code to implement Blockchain in Merkle Trees. 2.6 Java Code to implement Mining using Blockchain.	II to V	36
3	Prepare a detailed case study on any two known implementations of Blockchain.	I and IV	8
		TOTAL	56 Hrs.

Note

- Practical Exercises** may be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.
- The following are some **sample** 'Process' and 'Product' related skills (may be added/deleted depending on the course) that occur in the above listed **Practical Exercises** of this course required which are embedded in the COs and ultimately the competency.

Sr. No.	Sample Performance Indicators for the PrOs	Weightage in %
1	Preparing a logic to solve the problem.	30

2	Implement the logic with suitable/suggested programming language.	15
3	Identify and remove bugs.	10
4	Comparing the final output with existing solution and improvise the solution if needed.	20
5	Completing the tasks within time limit.	25
Total		100

6. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

These major equipment with broad specifications for the PrOs is a guide to procure them by the administrators to usher in uniformity of practical in all institutions across the state.

Sr. No.	Equipment Name with Broad Specifications	PrO. No.
1	Any standard computing hardware capable of executing standard programming languages like java, python, C etc. Open-source software should be preferred.	ALL

7. AFFECTIVE DOMAIN OUTCOMES

The following **sample** Affective Domain Outcomes (ADOs) are embedded in many of the above-mentioned COs and PrOs. More could be added to fulfil the development of this competency.

- a) Follow ethical practices.
- b) Work as a leader/a team member.

The ADOs are best developed through the laboratory/field-based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

- i. 'Valuing Level' in 1st year ii.
- 'Organization Level' in 2nd year. iii.
- 'Characterization Level' in 3rd year.

8. UNDERPINNING THEORY

Only the major Underpinning Theory is formulated as higher level UOs of *Revised Bloom's taxonomy* in order development of the COs and competency is not missed out by the students and teachers. If required, more such higher level UOs could be included by the course teacher to focus on attainment of COs and competency.

Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
------	--	-----------------------

UNIT-I Introduction to Blockchain and distributed ledgers.	1.a Explain Blockchain and distributed ledger. 1.b Explain asymmetric key encryption. 1.c Describe CAT theorem in Blockchain.	1.1 Introduction to Blockchain and distributed ledger. 1.2 Application, limits, and challenges of Blockchain. 1.3 basics of Cryptography: public key, private key, asymmetric encryption model, Hashing, signature schemes and elliptic curve cryptography. 1.4 Consistency, Availability, and Partition Tolerance in Blockchain.
UNIT-II Structure of Blockchain	2.a Examine the type of Blockchain architecture. 2.b Describe components of Blockchain. 2.c Apply concept of asymmetric key encryption. 2.d Explain decentralized network.	2.1 Types of Blockchain: Public and private; permissioned and permission less; tokenized and token less Blockchain. 2.2 Sidechain. 2.3 Core Components of Blockchain. 2.4 Distributed identity: Public and private keys, Digital identification, and wallets. 2.5 Decentralized network, Distributed ledger. 2.6 Data structure of a Blockchain.
UNIT-III Essentials of Blockchain	3.a Explain consensus mechanism in Blockchain. 3.b Describe Proof or Works(PoW) and block reward. 3.c Examine type of attacks in Blockchain.	3.1 Consensus mechanisms in Blockchain. 3.2 Confirmation and finality: The limits of proof-of-work, alternative of proof of work. 3.3 block rewards and miners and difficulty under competition. 3.4 Forks and consensus chain. 3.5 Sybillattacks and the 51% attack.
Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
UNIT –IV Conceptualization of Blockchain as cryptocurrency	4.a Describe bitcoin. 4.b describe consistency and fault tolerance. 4.c Apply concept of cryptography. 4.d Describe implementations of Blockchain in cryptocurrency.	4.1 Bitcoin: Merkle tree and bitcoin. 4.2 Bitcoin and the Eventual Consistency, Byzantine fault tolerance. 4.3 Bitcoin and secure hashing, bitcoin blocksize, bitcoin mining. 4.4 Proof of Work, Bitcoin Scripting. 4.5 Blockchain collaborative implementations: Hyper ledger, corda- ERC 20 and token.
UNIT-V Decentralization using Blockchain	5.a Describe smart contract. 5.b Describe decentralization in Blockchain application.	5.1 Blockchain and full decentralization, smart contract. 5.2 Decentralized autonomous organization (DAO). 5.3 Decentralized applications

Note: The UOs need to be formulated at the 'Application Level' and above of 'Revised Bloom's Taxonomy' to accelerate the attainment of the COs and the competency.

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
1	Introduction to Blockchain and distributed ledgers	8	4	6	4	14
2	Structure of Blockchain	10	2	10	4	16
3	Essentials of Blockchain	8	4	8	2	14
4	Conceptualization of Blockchain as cryptocurrency	10	4	8	6	18
5	Decentralization using Blockchain	6	2	4	2	8
Total		42	16	36	18	70

Legends: R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)

Note: This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related **co-curricular** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidence for their (student's) portfolio which will be useful for their placement interviews: a) Give a presentation on relevant topics.

b) Visit a relevant company and discuss their practices adopted for development.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

- Massive open online courses (**MOOCs**) may be used to teach various topics/subtopics.
- Guide student(s) in undertaking micro-projects.
- 'L' in section No. 4** means different types of teaching methods that are to be employed by teachers to develop the outcomes.
- About **20% of the topics/sub-topics** which are relatively simpler or descriptive in nature is to be given to the students for **self-learning**, but to be assessed using different assessment methods.
- With respect to **section No.11**, teachers need to ensure to create opportunities and provisions for **co-curricular activities**.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her at the beginning of the semester. In the first four semesters, the micro-project is group-based. However, in the fifth and sixth semesters, it should preferably be **individually** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In situations where groups are formed for micro-projects, the number of students in the group should **not exceed four**. The microproject could be industry application based, internet-based, workshop-based, laboratorybased, or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions to the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than **16 (sixteen) student engagement hours** during the course. The student ought to submit a micro-project by the end of the semester to develop the industry-oriented COs. A suggested list of micro-projects is given here. This must match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

Sample1: Do a feasibility analysis on Vote chain – Electronic Voting System based on Blockchain and prepare a detailed plan to create the system.

Sample2: Do a feasibility analysis on Transparent and Genuine Charity Applications based on Blockchain and prepare a detailed plan to create the system.

Sample3: Do a feasibility analysis on Identifying fake products through a barcode based Blockchain system and prepare a detailed plan to create the system.

Sample4: Do a feasibility analysis on Blockchain-based Land Registries System and prepare a detailed plan to create the system.

13. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication with place, year and ISBN
1	"Mastering Bitcoin: Unlocking Digital Cryptocurrencies"	Andreas Antonopoulos	O'Reilly Media, Inc. 2014.
2	"Block chain"	Melanie Swa	O'Reilly Media 2014
3	Blockchain Technology	Kumar Saurabh	Wiley, 2020, ISBN 978-8126557660

14. SOFTWARE/LEARNING WEBSITES: □

Suggested Software:

- Latest version of JDK,
- Latest version of Python Interpreter, ○ Compiler/interpreter of any programming language.

□ Learning Resources:

- **Course Name:** Blockchain and its Applications By Prof. Sandip Chakraborty, Prof. Shamik Sural **Portal/Website:** NPTEL. ○ **Course Name:**

Cryptocurrency and Blockchain: An Introduction to Digital Currencies By Richard B. Worley **Portal/Website:** MyMOOC.

- **Course Name:**Blockchain Basics By Bina Ramamurthy **Portal/Website:** Coursera.

15. PO-COMPETENCY-CO MAPPING

Semester VI	Foundation of Blockchain (4361603)						
	POs and PSOs						
Competency & Course Outcomes	PO1 Basic & discipline specific knowledge	PO2 Problem Analysis	PO3 Design / development of solutions	PO4 Engineering Tools, Experimentation Testing	PO5 Engineering practices for society, sustainability & environment	PO6 Project Management	PO7 Lifelong learning
Competency							
Understand concepts of cryptography, Blockchain and distributed ledger.	2	1	1	1	-	-	1
Categorize Blockchain structure and Blockchain types.	2	2	1	1	-	-	1
Examine Consensus mechanism and attack types in Blockchain.	2	3	2	2	-	-	1
Apply concepts of cryptography and Blockchain in cryptocurrency.	1	1	3	2	-	1	1
Understand decentralization with the help of Blockchain.	2	2	1	1	-	-	1

Legend: '3' for high, '2' for medium, '1' for low or '-' for the relevant correlation of each competency, CO, with PO/ PSO

16. COURSE CURRICULUM DEVELOPMENT COMMITTEE

GTU Resource Persons

Sr. No.	Name and Designation	Institute	Email
1	Mr. Nandu A. Fatak(HOD)	Govt. Polytechnic for Girls, Ahmedabad	Nandu_fatak@gmail.com
2	Mr. Vimal L. Vachhani	Govt. Polytechnic for Girls, Ahmedabad	vimal.l.vachhani@gmail.com
3	Mr. Henish H. Shah	Govt. Polytechnic for Girls, Ahmedabad	henish.it.dte@gmail.com