COURSE DESCRIPTION

Blockchain Fall - 2024

Course Code	CS 520
Course Title	Block chain
Credit Hours	3
Prerequisites by Course(s) and Topics	N/A
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	Midterm Exam 20% Quizzes 15% Assignments / Project (Phases) 30% Final Exam 35% "Weightage could be changed as per Instructor's direction.
Course Coordinator	Dr. Umar Janjua
Professor's Contact	Email: umar.janjua@itu.edu.pk
Current Catalog **Description**	
Textbook	Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder with a preface by Jeremy Clark
Course Goals	This course focuses on the foundational technologies behind blockchain. We will cover the concepts of distributed ledger, consensus mechanisms, authentication techniques, and relevant protocols. The course will provide case studies of blockchain applications such as cryptocurrencies.
Topics Covered in the Course	**Introduction** What is Blockchain? ,How Bitcoin is related to Blockchain, History of Bitcoin How Bitcoin Works Transactions, Blocks, Mining, and the Blockchain , Bitcoin Transactions Keys, Addresses Public key Cryptography and crypto currency , Bitcoin Addresses, Key Formats of Implementing Keys and Addresses in Python, Advanced Keys and Addresses, Vanity Addresses

	Wallets Wallet Technology Overview, Random Wallets , Wallet Technology Details **Transactions** Introduction , Transactions in Detail , Transactions Outputs and Inputs, Transactions Fees , Transaction Scripts and Script Language, Turing Incompleteness, Digital Signatures (ECDSA), How Digital Signatures work, Verifying the Signature , Bitcoin Addresses, Balances, and Other **Advanced Transactions and Scripting** Introduction , Multi signature , Pay-to-Script-Hash (P2SH) , Data Recording Output (RETURN) , Time locks , Scripts with Flow Control (Conditional Clauses) , Complex Script Example **The Bitcoin Network** Peer-to-Peer Network Architecture , Bloom Filters, SPV Nodes and Privacy , Encrypted and Authenticated Connections , Transaction Pools **The Blockchain** Introduction, Structure of a Block, Block Header , Block Identifiers: Block Header Hash and Block Height , Merkle Trees , Bitcoin's Test Blockchains **Mining and Consensus** Decentralized Consensus, Proof-of-Work Algorithm, Mining pools Bitcoin Security Security Principles, Physical Bitcoin Storage, Hardware wallets **Blockchain Applications** Building Blocks (Primitives), Applications from Building Blocks, Colored Coins **Zero-Knowledge Proofs (ZKP)** Introduction to ZKP Types of ZKP: ZK-SNARKs, ZK-STARKs, Z-cash, Defi (Decentralized Finance) 2.0, NFTS

	Other Blockchain Implementations Introduction to Ethereum , Consensus Attacks ,Changing the Consensus Rules, Hard Forks , Soft Fork Signaling with Block Version , Consensus Software Developments **Solidity** Ethereum, Solidity language, implementation of Smart contracts, vulnerabilities in solidity smart contracts and their mitigation.
Programming Assignments Done in the Course	**Project is given to students in which they will work on real projects with Blockchain lab RA on Blockchain platforms.**