ABHYASMITRA.IN

COMPREHENSIVE UNIVERSITY STUDY NOTES

BLOCKCHAIN TECHNOLOGY

Unit II — Cryptocurrency, Bitcoin & Blockchain Platforms

Topics Covered in this Unit

Introduction to Bitcoin & Cryptocurrency: Double-Spending Solution & Nakamoto Consensus
Bitcoin Transactions & The UTXO Model: Inputs, Outputs, Change Addresses vs. Account-Based Systems
Bitcoin Scripting: Stack Execution, Non-Turing Completeness & P2PKH / P2SH Script Evaluation
Wallets & Key Hierarchies: Private Key -> Public Key -> Base58Check Address Derivation Pipeline
Deterministic Wallets (BIP-32 / BIP-39 / BIP-44): Mnemonic Phrases, HD Trees & Hot vs. Cold Storage
The Bitcoin Mining Process: Nonce Search, Target Difficulty Adjustment & Halving Economics (21M Cap)
Blockchain Security Attacks: 51% Hashrate Attack, Sybil Attack, Double-Spending & Selfish Mining
Cryptocurrency Economics & Tokenomics: Deflationary Dynamics, Gas Economics & Transaction Fees
Comparative Analysis of Blockchain Platforms: Bitcoin, Ethereum, Hyperledger Fabric, IOTA & R3 Corda
High-Yield University Exam Question Bank with Detailed Model Answers & Unit Summary

Compiled in a structured, easy-to-understand, textbook style format
Specially curated for B.Tech / B.E. / BCA / MCA / B.Sc Computer Science & IT Students

COURSE SYLLABUS & MAPPING

[UNIT II SYLLABUS — PRESCRIBED UNIVERSITY CURRICULUM]

This section contains the official syllabus for Unit II. Verify with your university curriculum mapping.

Unit II Syllabus Breakdown:

Unit II - Cryptocurrency and Bitcoin: Introduction: Bitcoin and the Cryptocurrency, Cryptocurrency, Bitcoin Transactions and Scripts, Wallets and Keys, Mining Process, Blockchain Security Mechanisms, Cryptocurrency Economics. Types of Cryptocurrency: Cryptocurrency Usage, Cryptowallets: Metamask, Coinbase, Binance. Types of Blockchain Platforms: Bitcoin, Ethereum, Hyperledger, IoTA, Corda, and R3.

• Course Code: _____ • Semester / Year: _____

TABLE OF CONTENTS

2.1 Bitcoin, Cryptocurrencies & The UTXO Model

Definition: Bitcoin (Satoshi Nakamoto, 2008)

Bitcoin is a decentralized, peer-to-peer electronic cash system that solves the Double-Spending Problem without relying on a central banking authority by combining Proof of Work consensus, cryptographic hash chaining, and digital signatures.

The Unspent Transaction Output (UTXO) Model vs. Account-Based Model

Comparison Dimension	UTXO Model (Bitcoin, Cardano)	Account-Based Model (Ethereum, Solana)
Core Concept	Transactions consume discrete, immutable Unspent Transaction Outputs (UTXOs) as inputs and produce new UTXOs as outputs.	Maintains global state accounts with updating account balances (similar to a traditional bank balance).
Transaction Verification	Stateless verification: validators only check if referenced UTXOs exist in the active UTXO set and are unspent.	Stateful verification: validators must look up current account balance from the global state trie.
Parallel Processing	High: non-interfering transactions spending distinct UTXOs can be verified completely in parallel.	Low: transactions affecting the same account must be executed sequentially to prevent race conditions.
Privacy	Superior: encourages generating a brand-new change address for every single transaction.	Inferior: all transactions associate with a static public address, simplifying address clustering.

Bitcoin Transactions & Script Execution (P2PKH)

Bitcoin uses a Forth-like, stack-based, non-Turing complete scripting language. It intentionally omits loops and recursion to guarantee termination and prevent infinite-loop Denial-of-Service attacks on validator nodes.

- **Standard P2PKH (Pay-to-Public-Key-Hash) Script Execution:**
  - ScriptPubKey (Locking Script on UTXO): OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
  - ScriptSig (Unlocking Script on Input): <Signature> <PublicKey>
  - Combined Execution on Stack: [<Sig> <PubKey> OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG]. Evaluates to TRUE (1) if the signature is authentic!

2.2 Wallets, Keys & Address Generation Pipeline

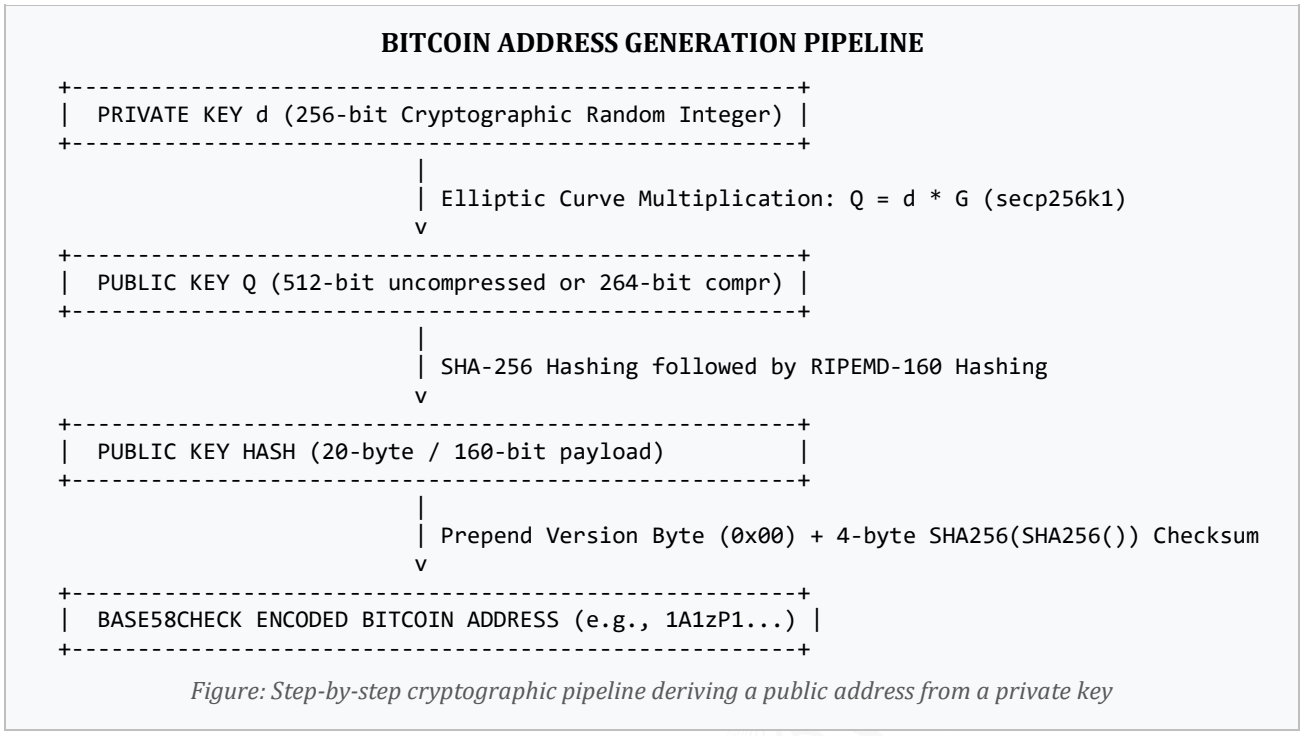

Figure: Step-by-step cryptographic pipeline deriving a public address from a private key

Wallet Categories & Deterministic Standards (BIP-32 / BIP-39 / BIP-44)

- **1. Hot Wallets vs. Cold Wallets:** Hot Wallets (MetaMask, Coinbase app) remain connected to the Internet (convenient for DApps, higher attack surface). Cold Wallets (Hardware Ledger, Trezor, Paper) store private keys air-gapped from the Internet (maximum security).
- **2. BIP-39 (Mnemonic Seed Phrases):** Converts a 128-to-256 bit random seed into 12 or 24 human-readable words chosen from a standardized 2048-word dictionary with a built-in checksum.
- **3. BIP-32 & BIP-44 (Hierarchical Deterministic HD Wallets):** Enables deriving an infinite tree of child private/public key pairs from a single Master Seed via derivation path: m / purpose' / coin_type' / account' / change / address_index (e.g., Bitcoin: m/44'/0'/0'/0/0; Ethereum: m/44'/60'/0'/0/0).

2.3 The Mining Process, Halving & Security Attacks

1. Proof of Work (PoW) Mining Mechanics

Miners bundle unconfirmed transactions from the Mempool into a candidate block. Mining involves finding an arbitrary 32-bit Nonce such that the double-SHA256 hash of the 80-byte block header falls strictly below the network Target Difficulty:

- **Mining Condition:** SHA256(SHA256(Block_Header)) < Target

- **Difficulty Adjustment Algorithm:** Every 2,016 blocks (~14 days), the network automatically recalibrates Difficulty: New_Difficulty = Old_Difficulty * (Actual_Time_for_2016_Blocks / 20160_minutes). Guarantees a steady 10-minute block interval!
- **Halving Economics & 21 Million Hard Cap:** Miners receive the Coinbase Block Reward plus transaction fees. Block rewards halve every 210,000 blocks (~4 years): 50 -> 25 -> 12.5 -> 6.25 -> 3.125 BTC. Total supply is mathematically capped at 21,000,000 BTC.

2. Major Blockchain Security Attacks

- • **51% Attack (Majority Hashrate Takeover):** An adversary controlling > 50% of the total network hashing power can outpace the honest chain, executing double-spends and reorganizing historical blocks.
- • **Sybil Attack:** An attacker creates thousands of fake virtual nodes to monopolize network communication and isolate honest nodes. Mitigated by Proof of Work / Proof of Stake (requiring scarce physical/economic resources to participate).
- • **Selfish Mining (Eyal & Sirer, 2014):** A mining pool withholds privately discovered valid blocks and releases them strategically to invalidate honest miners' work, earning disproportionate revenue.

2.4 Types of Blockchain Platforms: Comparative Analysis

Platform	Platform Type	Consensus Algorithm	Smart Contract Language	Key Characteristic & Architecture
Bitcoin	Public / Permissionless	Proof of Work (PoW - SHA256)	Bitcoin Script (Non-Turing complete)	Digital gold; UTXO transaction model; 10-minute blocks; 7 TPS.
Ethereum	Public / Permissionless	Proof of Stake (PoS - Casper)	Solidity, Vyper (Turing complete EVM)	Global decentralized computer; Account-based model; DeFi & NFTs.
Hyperledger Fabric	Private / Permissioned	Pluggable (Raft, PBFT, BFT)	Chaincode (Go, Java, Node.js)	Enterprise modular DLT; private channels; zero cryptocurrency token required.
IOTA	Public IoT Network	Tangle (Directed Acyclic Graph - DAG)	N/A (Micro-transactions)	Zero transaction fees; scalable IoT device data streams; no blocks or miners.

Platform	Platform Type	Consensus Algorithm	Smart Contract Language	Key Characteristic & Architecture
R3 Corda	Consortium / Enterprise	Notary Clusters (Raft / BFT)	Kotlin, Java (JVM-based)	Point-to-point state sharing (no global broadcast); designed for regulated banking.

2.5 High-Yield University Exam Question Bank

Part A: Short Answer Questions (2 to 5 Marks)

Q1. What is the UTXO model? How does it differ from the Account model? [3-4 Marks]

- **Answer:** UTXO (Unspent Transaction Output) models transactions as discrete cash notes consumed as inputs and generating new unspent outputs. In contrast, the Account model (Ethereum) maintains global accounts with updating balances, enabling simpler smart contracts but requiring sequential state updates.

Q2. Explain the Bitcoin Difficulty Adjustment mechanism. [3 Marks]

- **Answer:** Every 2,016 blocks (~14 days), the network calculates the ratio of actual time taken versus the expected 20,160 minutes. Target difficulty is multiplied by this ratio, ensuring that block generation time remains constant at ~10 minutes regardless of changes in global hashrate.

Q3. What is a 51% Attack? What can and cannot an attacker do? [4 Marks]

- **Answer:** Controlling > 50% hashrate allows an attacker to create a longer private chain to reverse recent transactions (double-spending) and block confirmations. The attacker CANNOT steal funds from other accounts or forge digital signatures because ECDSA cryptography remains intact.

Part B: Long Answer Questions (10 to 15 Marks Outline Guides)

- **Q4. Trace the complete Bitcoin Address Derivation pipeline from 256-bit Private Key to Base58Check Address with all hashing steps. [12 Marks]**
- **Q5. Explain the Bitcoin Mining Process, Proof of Work equation, Coinbase reward, 4-year halving cycle, and the 21M total supply cap. [12 Marks]**
- **Q6. Compare Bitcoin, Ethereum, Hyperledger Fabric, IOTA, and R3 Corda across consensus, smart contracts, throughput, and enterprise suitability. [12 Marks]**
- **Q7. Explain Hierarchical Deterministic (HD) Wallets, BIP-39 mnemonic seed phrases, and BIP-44 key derivation paths. [10 Marks]**

2.6 Unit Summary & Key Takeaways

- Bitcoin utilizes the UTXO model where transactions consume unspent outputs validated via Forth-like Script (P2PKH).
- Public addresses are derived through ECC point multiplication, SHA-256, RIPEMD-160, and Base58Check encoding.
- HD wallets (BIP-32/39/44) derive infinite key hierarchies from a single 12/24 word mnemonic seed phrase.
- Proof of Work mining searches for a nonce satisfying double-SHA256 < Target, dynamically adjusted every 2,016 blocks.
- Bitcoin block rewards halve every 210,000 blocks until reaching the 21,000,000 BTC hard cap.
- Blockchain platforms range from public networks (Bitcoin, Ethereum) to enterprise permissioned frameworks (Hyperledger Fabric, R3 Corda) and DAGs (IOTA).