**Day 1: Progress Report – Blockchain Learning**

Completed 4 lectures covering the following core topics:

* Centralized, decentralized, and distributed systems
* Definition and structure of blockchain
* Hash functions, digests, and Merkle trees
* Miners and smart contracts
* Block structure and transaction data
* Block hashes and their significance
* Permissioned vs. permissionless blockchains
* Challenge–response in consensus mechanisms
* Provenance tracking in data
* IPFS and the distributed web

**Day 2: Progress Report – Blockchain Learning**

**Lectures Covered:** Lecture 5 to Lecture 9 (5 lectures)

**Focus:** Cryptographic foundations and Bitcoin fundamentals

**Core Topics Learned:**

**🔐 Cryptographic Foundations**

* Cryptographic Hash Functions  
  • Properties: Collision Resistance, Pre-image Resistance, Avalanche Effect, Puzzle-Friendliness  
  • Introduction to the SHA-256 algorithm
* Hash Pointers and Hashchains  
  • Concept of hash pointers as secure references to previous data  
  • Use of hashchains in ensuring data integrity

**🌲 Merkle Trees**

* Structure and purpose in efficient data verification
* Use in blockchain for verifying large transaction sets efficiently

**✍️ Digital Signatures & Public Key Cryptography**

* Purpose of digital signatures in verifying authenticity
* Public and Private Key Mechanism  
  • Public Key (used for encryption)  
  • Private Key (used for decryption)
* RSA Algorithm: Basics of public key encryption
* Digital Signing Workflow  
  • Signing with private key, verification with public key  
  • Efficiency via signing the hash (digest) instead of full message

**💰 Cryptocurrency Concepts**

* Introduction to Cryptocurrency secured by hashchains and digital signatures
* **Bitcoin Basics**  
  • Coin creation and supply  
  • Sending payments  
  • Double spending problem and blockchain’s solution  
  • Anonymity in Bitcoin

**📜 Bitcoin Script**

* Introduction to Bitcoin’s scripting language (similar to Forth)  
  • Stack-based, uses postfix notation  
  • Common instructions and examples of real-world Bitcoin scripts

**🌐 Bitcoin P2P Network**

* Joining the Bitcoin peer-to-peer network
* Transaction broadcast (flooding mechanism)
* Mining and block generation  
  • Mining puzzle and Proof-of-Work  
  • Block flooding and propagation  
  • Consensus via longest valid chain  
  • Handling latency in block propagation