**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

**Day 3 Progress Report – Blockchain Learning**

Lecture covered: 10 to 13 (4 lectures)

1. Consensus
2. why Consensus
3. example
4. why it can be difficult in certain scenarios
5. Distributed consensus
   1. Faults in distributed systems
      1. Crash fault
      2. Network/portioned fault
      3. Byzantine fault
   2. Properties
      1. Termination
      2. Validity
      3. Integrity
      4. Agreement
6. Synchronous vs Asynchronous system
   1. Asynchronous system
      1. FLP85
   2. Synchronous system
      1. Paxos
      2. Raft
      3. Byzantine fault tolerance (BFT)
7. Correctness of distributed consensus protocol
   1. Safety
   2. Liveliness
8. Consensus in an open system
   1. Traditional distributed consensus protocol
      1. Message passing
      2. Shared memory
9. Consensus in a bitcoin network
10. Consensus algorithm in bitcoin
    1. PoW
       1. Cryptographic hash as PoW
       2. Hashcash PoW
11. Bitcoin Proof of Work
    1. Solving the double spending problem
12. Sybil attack
13. DOS (denial of services) attack
14. Breaking bitcoin PoW
    1. The monopoly problem
    2. PoW power consumption
15. Handling monopoly and power consumption – proof of stake(PoS)
16. PoS (Proof of stake)
    1. Variant of stake
17. PoB (proof of burn)
18. Difference between PoW, PoS and PoB
19. PoET (Proof of elapsed time) {intel}
    1. PoET over trusted environments
20. Mining bitcoins
    1. The life of a miner
    2. Mining difficulty
    3. Setting the difficulty
    4. Hash rate vs difficulty
    5. Mining hardware
    6. Mining pool methods
       1. Pay per share (PPS)
       2. Proportional
       3. Pay per last N share (PPLNS)
       4. Pros and cons