| Course Code | Course Title |
|---|---|
| **COMP 4541** | **Blockchain, Cryptocurrencies and Smart Contracts** |

Course Description

This course provides a holistic introduction to Blockchain Protocols and Smart Contracts. The students will learn how cryptocurrencies such as Bitcoin and Ethereum work, why they are secure, and how they can be used to implement real-world financial contracts without relying on trusted third-parties or centralized control. They will also learn to avoid, detect, and fix common security vulnerabilities in smart contracts.

List of Topics

1. Introduction to Cryptocurrencies and Decentralization
2. Hash Functions and Public-key Cryptography
3. The Double-spending Problem
4. Bitcoin and Proof-of-Work (PoW)
5. Proof-of-stake and other alternatives to PoW
6. Programmable Blockchains
7. Introduction to Ethereum and Solidity
8. Tools for Implementing Smart Contracts
9. Commitment Schemes
10. Auctions and Escrows
11. Re-entrancy and Out-of-gas Vulnerabilities
12. Incentivization Bugs and Attacks by Miners
13. Verifying Correctness of Smart Contracts

Textbooks

N/A

Assessment Approach and Weight

| | |
|---|---|
| 4 Homeworks (10% each) | 40% |
| Individual project | 30% |
| Final exam | 30% |
| Total | 100% |