Blockchain and Digital Currencies

Lecture 0

PHBS 2024 M3

Syllabus

- Class:
  - Lectures: Tuesday and Friday 8:30 – 10:20 AM
  - Location: 319
- Instructor: Haiyang Zheng
  - Email: hyzheng@phbs.pku.edu.cn
  - Office: PHBS Building, Room 736
  - Office Hour: Monday & Thursday 8:30-9:30 and Wednesday 3-5pm
- Teaching Assistant: Chang Li 2nd year FinTech MA

Course Overview

- This course is an advanced course of blockchain technology and its application in various finance applications and digital currencies. This course focuses on technology details of blockchain and requires Java programming to simulate the mining process of a simple blockchain.

- The main topics include underlying working mechanisms for BitCoin blockchain and Etherum, DeFi, security and privacy issues on blackchain, etc.

References

- No official textbook

- There are four main references:
  - Bitcoin and Cryptocurrency Technologies https://bitcoinbook.cs.princeton.edu/
  - The lecture notes from Professor Zhen Xiao http://zhenxiao.com/blockchain/
  - The lecture notes of CS 294: Decentralized Finance at UC Berkeley: https://rdi.berkeley.edu/berkeley-defi/f22
  - The lecture notes of CS 251: Blockchain Technologies at Stanford: https://cs251.stanford.edu/syllabus.html

Tentative Schedule

lecture	date	topics	homework
1	2024/2/18	course overview, Hash pointer and Merkle Tree	
2	2024/2/21	Digital signatures and its application in transaction scripts	
3	2024/2/25	Application of transaction scripts	
4	2024/2/28	Double spending problem and proposed solutions	
5	2024/3/4	Scaling issues and lighting network of bitcoin blockchain	Homework #1
6	2024/3/7	Ethereum: account based ladger and accounts, EVM	
7	2024/3/11	Ethereum: status, transaction, and receipt trees	HW #1 due
8	2024/3/14	Ethereum: mining + uncle block + POS	Homework #2
9	2024/3/18	Ethereum: smart contracts + gas	
10	2024/3/21	Ethereum: smart contracts applications + solidity	
11	2024/3/25	**project research ideas/ review**	HW #2 due
12	2024/3/28	***midterm***	
13	2024/4/1	projects and DAO	**projects officially start**
14	2024/4/4	**Moved to 4/2** Midterm results and rest of DAO	
15	2024/4/8	DEX	
16	2024/4/11	DeFi and its security	
17	2024/4/15	Privacy on blockchain	
18	2024/4/18	***project presentation***	

Grading

- Attendance: 5% (final project presentations)
- Homework: 20%
- Midterm: 35% (tentative on 2025/3/28?)
- Project: 40%
- Grade in letters (e.g., A+, A-, ... ,D+, D, F).
  - No more than 30% can receive A+, A, and A-;
  - No more than 90% can receive B and above.
- Academic Honesty and Plagiarism
- No extra credits or makeup exams

Important Notes

- Prerequisites:

  Students should have good Java programming skills and have taken the Introduction to Fintech and Information Security courses.

- AI Tools Usage:

  Students are prohibited from using AI tools to generate code or complete reports/ppt for homework assignments and projects. However, students may use AI tools to assist in finding references, supplementing materials, and refining writing and formatting.

Guidelines for Submission and Emails

- Submit your homework via email with title
  - 2024.M3.Blockchain YourName Homework_1
  - Homework file with the same name
- For project submission
  - 2024.M3.Blockchain YourName ProjectGroup_#
  - Project materials compressed into one ZIP file with the same name
- For email questions, please make the title
  - 2024.M3.Blockchain YourName QuestionTitle