

"The Blockchain: Theory and Practice"

Course Detail

Course Title: "The Blockchain: Theory and Practice"

Credit: 1 Credit (CS5543)

Course Coordinator: Kotaro Kataoka

Course Sponsor: Chaintope Inc.

Course Period: September 17th to September 22nd (5:30 pm - 8:00 pm)

Prerequisite: Basics on Operating System, Computer Networks, VM Operation and Programming

Overview

This course explains the underlying mechanism of blockchain and provides the necessary knowledge needed for starting blockchain programming. Although blockchain is a relatively new technology created to realize cryptocurrency, it has a lot of potentials to transform existing security models based on P2P, and various applications are going to emerge out of this.

This course first introduces the outline of blockchain with the background of the cryptocurrency being born. After that, it delves into Bitcoin that was the first cryptocurrency to use blockchain. Students will understand its basic cryptographic knowledge, detailed data structure and remittance transactions using digital signatures. Besides, we will also explore essential topics such as blockchain security and incentive design to maintain the P2P network. In the hands-on assignment, students create programs to send transactions on Bitcoin blockchain and deepen their fundamental understanding through actual cryptocurrency remittances in testnet.

The blockchain is still in the developing stage, and various improvements are being researched and proposed. For this reason, it is also the target to learn the latest topics while organizing the possibilities and challenges of the blockchain. After completing this course, students can gain essential skills in programming blockchains and necessary knowledge to tackle more advanced topics.

References

[1] Mastering Bitcoin, 2nd Edition by Andreas M. Antonopoulos, ISBN-13: 978-1491954386, O'Reilly Media, 2017.

Tentative Timetable

Day 1: 5:30 pm – 8:00 pm (2.5 hrs)

- Evolution of currency
- Overview of Blockchain
- (Hands-on) Preparing Bitcoin Core on Docker

Day 2: 5:30 pm – 8:00 pm (2.5 hrs)

- The structure of Bitcoin and roles of each nodes
- Basic usage of cryptocurrency
- (Hands-on) Working with Bitcoin Core using CLI

Day 3: 5:30 pm – 8:00 pm (2.5 hrs)

- Details of blocks and transactions
- Address, signatures and script
- (Hands-on) Creating simple transaction from scratch

Day 4: 5:30 pm – 8:00 pm (2.5 hrs)

- Security: Double spent, 51% attack, forking, private key management, multi-signature
- Scalability: Bottlenecks and its trade-offs
- (Hands-on) Trying to do double spend and so on

Day 5: 5:30 pm – 8:00 pm (2.5 hrs)

- To Upgrade the cryptocurrency: Colored Coins, Layer 2
- Possibility of decentralized applications: Ethereum and so on
- (Hands-on) Issue Openassets tokens on Blockchain

Day 6: 5:30 pm – 8:00 pm (2.5 hrs)

- Advanced and cutting-edge topics of blockchain
- Conclusion
- Examination

Assignments

- Create basic Bitcoin wallet application
- (Advanced) Multisig wallet
- (Advanced) Uni-directional micro payment channel

Remarks

The course schedule would be adjusted according to the progress and situations.