Blockchain and Future Society 2018

SYLLABUS								
Classification	Graduate School	**Course No.**	IC5xxxx	**Hrs:E:Credits**	3/1/3	**Instructor**	Lee, Heung-No	
Course Title	Korean	**블록체인과 미래사회**						
	English	**Blockchain and Future Society**						
Course Outline	This course aims to give an introduction to blockchain technology and its applications. Blockchain applications of interest include cryptocurrencies, governance and vote systems, transfer of rights and patents, and prosuming of energy/data and other valuable commodities. A detailed coverage of Bitcoin and Ethereum system will be given. At the end of the course, the students will be able to program and run their own version of blockchain system for an application of their own interest.							
Prerequisite	C/C++/Python							
Textbook/ References	Points to reference materials will be given inside class.							
Etcetera	Flipped learning via online lectures such as Coursera courses, i.e., Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Princeton University, and Youtube materials will also be utilized for certain parts of the lecture.							

Weekly Course Schedule

Week	**Description**	***Remarks**
1st	Introduction to Bitcoin	
2nd	Transactions, Timestamp, Bitcoin Network	
3rd	Incentive and Decentralization Mechanism of Bitcoin	HW#1 due
4th	How to Store and Use Bitcoins	
5th	Secure Hash Functions and Mining	HW#2 due
6th	Bitcoin Privacy	
7th	Possible Attacks and Counter Measures	
8th	Alternative Mining Puzzles (Coursera)	Bitcoin Project 1 due
9th	Altcoins and Cryptocurrency Ecosystem (Coursera)	
10th	Blockchain Platform	
11th	Introduction to Ethereum System	HW#3 due

12th	Token Economy	
13th	Smart Contracts	HW#4 due
14th	Blockchain Applictions	
15th	Community, Politics, Social Impacts	
16th	Regulations and Law	Final Project Due

What is Blockchain?

Blockchain is a new way of making transactions over the internet without the involvement of a third party such as banks and states. Currently, transactions such as transfer of ownership to a property and transfer of money are made via involvement of a trusted third party. Blockchain is a new cryptographically secure transaction record management system which has enabled the transfer of rights over internet without the third party. The role of trusted third party is to oversee the process of ownership transfer in any transaction. First, it makes sure that the seller holds the righteous ownership to the property in the transaction. Second, it checks to make sure that the seller does not spend the ownership to another party at the same time. Third, it provides a record in which the ownership right has moved from the seller to the buyer completely and permanently. In the blockchain technology, this process of transaction validation and record maintenance is done by a peer-to-peer network of anonymous computers with internet connection. The role of the trusted third party is given to this network of participating computers.

How Blockchain Works?

The p2p network of computers verifies each transaction, adds verified transactions to the permanent record, and keeps the record clean and safe from any faulty operation. A small chuck of transaction data, say 1 Mbyte and called a block, is timestamped and linked to the pre-existing chain of blocks in the chronological order. A new block containing a list of new verified transactions is added every ten minute to the chain. The verification is done by the peers in the network. In order to protect the chain from alteration and modification, the chain is announced and open in the network at all time and a proof-of-work is added to each block. This proof-of-work is a mathematical puzzle which has many possible solutions. A solution to this puzzle can only be found by guessing an input to a known function. Any computer can solve this puzzle but in average, it will take a very large amount of time, say one year or longer. The time to come up with a solution to this puzzle can be shortened, say within 10 minutes, when all the computers in the p2p blockchain network participate to solve this puzzle on their own. Blockchain provides an incentive to the first computer that solves the puzzle. This incentive attracts more members to join the race. The proof-of-work is then cryptographically added to a block. The chain of transactions is permanently linked to this chronologically chained proof-of-works. This implies if anyone or any group wishes to alter or modify any particular part of the chained data buried somewhere in the middle of the chain, then the person needs to recreate on its own all the proof-of-works made after that point of time. This requires an outpacing of all the computers who work together in the entire blockchain network and thus necessitates an enormous, if not impossible, amount of work done by the attacking party. Any attempt to modify the record stored in the chain becomes a

futile task for any one computer or group of computers to accomplish, unless the size of the attacking group is more than half the size of the p2p network of computers behaving normally.

Bitcoin and Ethereum?

Blockchain is the underlying infrastructure for Bitcoin and Ethereum. Bitcoin is the first crypto-currency. Ethereum is the first generalization of the Bitcoin to broader applications such as smart contracts and derivatives. The blockchain technology is anticipated to be the platform for new future industries for various purposes. Possible applications of the future include tracking ownership, digital assets, physical assets, and voting rights. Blockchain is however still too young and exploring the best ways in which it can be used should be the topic of discussion for the growing blockchain community as well as the society at large.

Some Recognition of Importance

- By 2025, 10 percent of global GDP will be stored on blockchain-related technology (World Economic Forum).
- Blockchain technology is envisioned to be utilized and help the two billion people worldwide who lack bank accounts (Bill & Melinda Gates Foundation)
- Goldman and Google Are Among the Most Active Blockchain Investors! (Bloomberg Technology, Oct. 18th, 2017)
- Watch out Google! Blockchain will set us free from data tyranny! (Thenextweb, Nov. 2017)

Course Objectives

- Comprehension of cryptocurrency concepts
- Understand the importance of blockchain technology
- Understand the bitcoin network
- Bitcoin transactions validated by miners
- Create and use bitcoin account effectively
- Understand Ethereum blockchain
- Deploy your own blockchain and see operation of your chains
- Discuss the compelling use-cases

Who should take this course?

This course is designed to give students the insights and hands-on programming knowledge to see the opportunities and innovations the blockchain technology will bring in to the society. In the world today, we often feel that innovation is not enough. As innovation continues, the lives of ordinary people have worsened, while small group of technological elites absorbs the majority of the social wealth created by new technologies. Needed are the abled students who are responsive to these problems, such as underemployment problems, income inequality, social barriers to opportunities, and disappearance of blue collar jobs. Blockchain is envisioned to be a solution to these inequalities problems of the market driven society. More harmonious and inclusive society can be built with creative use of the blockchain technology.