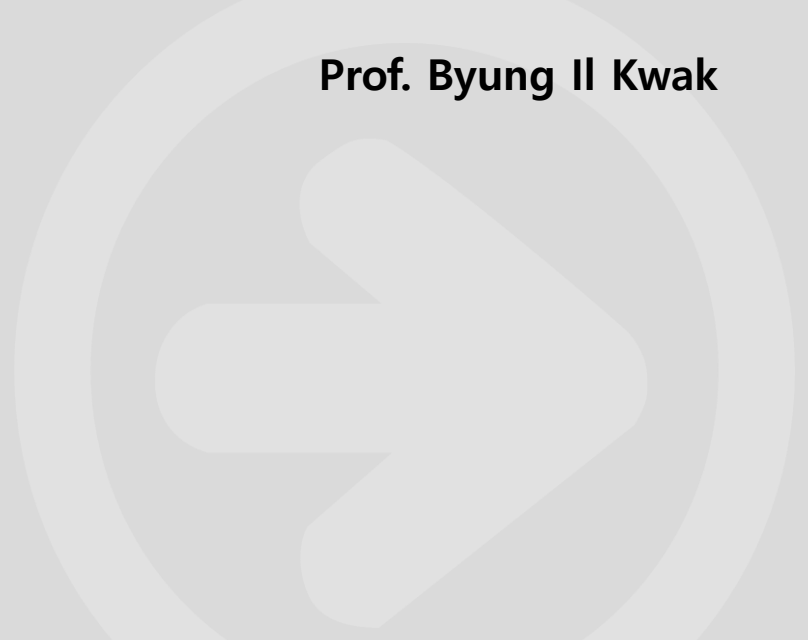




# Blockchain #1

course orientation and Introduction

Prof. Byung Il Kwak



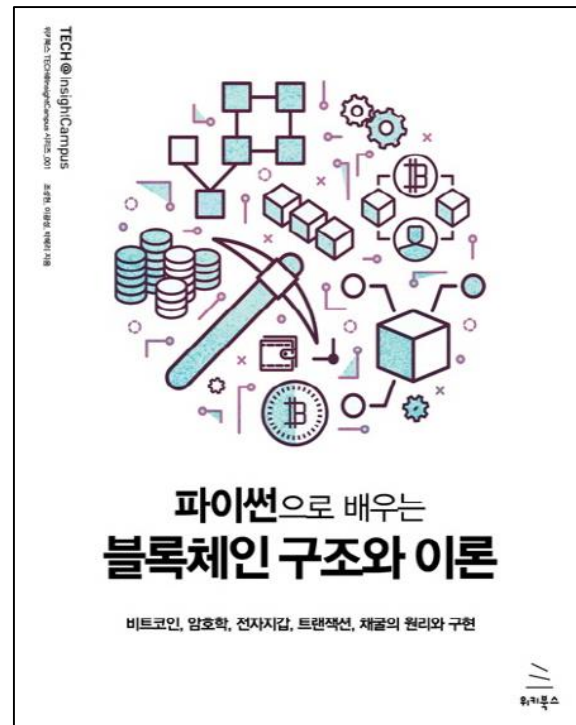
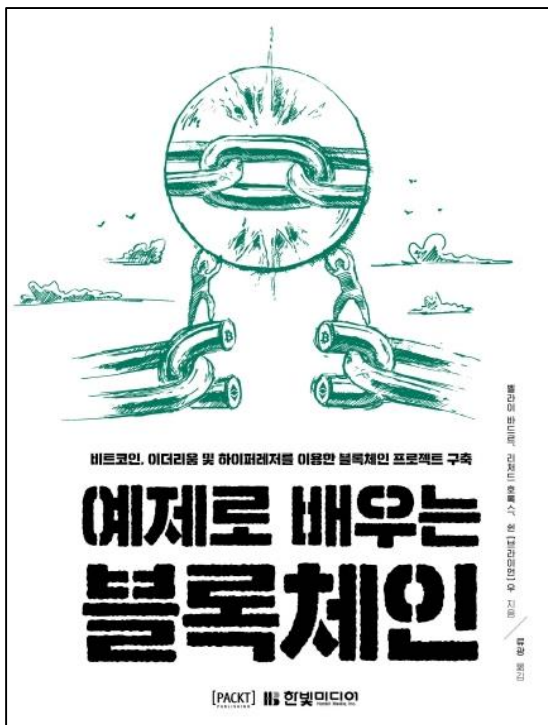
## □ 블록체인

- ▣ 블록체인의 기본 개념, 블록체인 플랫폼을 구성하는 핵심 기술인 해시함수, 공개키 암호, 디지털 서명 등의 암호기술, 블록과 블록체인의 구성 방법, 합의 알고리즘을 강의한다.
- ▣ 또한, 비트코인, 이더리움과 기반의 스마트 컨트랙트 기술을 이용한 실습을 수행한다.

# Course Introduction

## □ About textbook

- ▣ No textbook / Slide Notes
- ▣ 참고서적



# Course Introduction

회차	기간	학습 내용
1	08.30-09.03	블록체인 기능 (The basic features of blockchain)
2	09.06-09.10	블록체인의 기본 (The basics of blockchain)
3	09.13-09.17	블록체인의 역사 (The history of bitcoin and blockchain)
4	09.20-09.24	비트코인 (Bitcoin)
5	09.27-10.01	이더리움 (Ethereum)
6	10.04-10.08	지갑 (Wallet)
7	10.11-10.15	포크와 합의 (Fork and consensus)
8	10.18-10.22	중간고사
9	10.25-10.29	토큰 경제 (Token economy)
10	11.01-11.05	블록체인에서의 공격 (Attacks on blockchain)
11	11.08-11.12	스마트 컨트랙트 보안 (Smart contract security)
12	11.15-11.19	블록체인의 확장 (Blockchain extension)
13	11.22-11.26	이오스 (EOS: DPoS-based Altcoin)
14	11.29-12.03	ERC (Ethereum-based Token)
15	12.06-12.10	스마트 컨트랙트 개발 (Development tools for smart contract) - 강의 보충기간
16	12.13-12.17	블록체인의 한계 (Blockchain's limitation) - 강의 보충기간
17	12.20-12.24	기말고사

# Bitcoin & Cryptocurrencies









## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

(In October 2008, posted to the Cypherpunks mailing list)

# Bitcoin & Cryptocurrencies

# ▲	이름	가격	24h %	7d %	시가총액 ①	거래량 (24시간) ①	유통 공급량 ①	최근 7일
☆ 1	 Bitcoin BTC 구매하기	₩55,244,899.74	▲3.26%	▲3.29%	₩1,037,933,883,953,933	₩37,709,924,349,829 682,596 BTC	① 18,787,868 BTC	
☆ 2	 Ethereum ETH 구매하기	₩3,830,649.76	▲3.99%	▲4.91%	₩448,678,448,389,032	₩27,014,203,609,643 7,052,120 ETH	117,128,549 ETH	
☆ 3	 Binance Coin BNB 구매하기	₩501,650.98	▲6.92%	▲20.66%	₩84,346,108,114,367	₩2,648,755,651,087 5,280,077 BNB	168,137,036 BNB	
☆ 4	 Cardano ADA	₩2,519.00	▲2.79%	▲46.91%	₩80,890,540,782,978	₩5,785,703,660,815 2,296,827,268 ADA	① 32,112,187,324 ADA	

2021.08.16

# Evaluation Criteria

## □ Score Ratio

- ▣ Mid-term exam: 30%
- ▣ Final exam: 30%
- ▣ Assignments: 30%
- ▣ Others (*e.g.*, attendance): 10%

## □ FA rule

- ▣ 3지각: 1결석
- ▣ 6결석: F

## □ 휴강 / 보충

회차	휴강	보충
1	9월 20일 (월) - 추석연휴	12월 6일 (월)
2	10월 4일 (월) - 개천절 대체 공휴일	12월 9일 (수)
3	10월 11일 (월) - 한글날 대체 공휴일	12월 15일 (수)
4	11월 5일 (금) - 교내행사 관련 휴강	12월 16일 (목)
5	12월 3일 (금) - 교내행사 관련 휴강	12월 17일 (금)



## □ 과제 메일 리스트

- ▣ 수시과제 및 텀프로젝트 과제 관리를 위해 아래 email 주소를 사용
  - **swseckwak@gmail.com**
  - 과제 제출 시, 제출 이메일 또는 업로드 장소는 바뀔 수 있음
  - 과제 제출시
    - 제목: “[Blockchain]\_과제명\_학번\_이름”