

# ELEN E6883: An Introduction to Blockchain Technology

Blockchain, the underlying mechanism behind the bitcoin and other cryptocurrencies, is a revolutionary decentralized technology that is envisioned to be as impactful as internet. This course will introduce the technical foundations of blockchain and its applications to a wide range of industries including finance, computer science, supply-chain, smart power grid and social networking. The objective of this course is to provide students with required knowledge to conduct research on blockchain and basic skills to design smart contracts and implement distributed applications (DAPP).

## **Topics:** (each topic is covered by one or two lectures)

1. Background of blockchain and basic cryptography: hash functions, digital signatures, asymmetric encryption.

### Part I: Bitcoin Blockchain

2. Bitcoin and cryptocurrency technologies: bitcoin's consensus mechanism (i.e. Proof of Work) and its security achievement as a combination of technical methods and incentive engineering.

### Part II: Ethereum blockchain

3. Ethereum protocol and payment model for code execution
4. Smart contract: design and implementation
5. Decentralized Applications (DAPP): design and implementation

### Part III: Advanced blockchain technology

6. Alternative data structure to Bitcoin's blockchain: directed acyclic graph (DAG)
7. Proof-based consensus algorithms: proof of stake, proof of burn, proof of elapsed time, proof of luck.
8. Voting-based consensus algorithms: byzantine fault tolerance algorithms.
9. Case study: enterprise-level blockchains such as Hyperledger and Ripple

### Part IV: Blockchain ecosystem and applications

10. Initial coin offering (ICO) and regulations on blockchain
11. Applications to IoT, distributed AI, vehicular network, etc.

**Grading Policy (tentative):** homework (30%), exam (30%) and course project (40%).

**Pre-Requisites:** basic knowledge in probability, programming ability in some languages (e.g. C++, JavaScript).

## **References:**

1. Narayanan, Arvind, et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016. (pdf available on-line)
2. Academic papers and blockchain project whitepapers related to the above topics