ASU Online
Arizona State University

Engineering Blockchain Applications (CSE 598)

Note: The information and course outline below are subject to modifications and updates.

Course Description

Blockchain technology is revolutionizing digitalization prospects for many industries and emerging as an exciting and rapidly growing field. By detailing the architecture of the technology, this course ensures that learners will be well versed in blockchain fundamentals. At the same time, it is designed to put learners on the leading edge by presenting the abstract nature of blockchain technology and emphasizing its broad applicability. Topics include the mathematical and cryptographic underpinnings of the technology, as well as mining, consensus protocols, networking, and decentralized governance. This course also features an extended case study called “How It Works at Dash.”

Required Prior Knowledge and Skills

- Basic understanding of and coding experience with C++
- Proficiency in algebra

Course Learning Outcomes

Learners completing this course will be able to:

- Apply the Elliptic Curve Digital Signature Algorithm to identity management and computer security
- Determine the validity of chains given general consensus rules
- Determine whether changes in consensus rules for a Nakamoto network will result in a successful protocol fork
- Compare proof of work secured blockchains’ security to alternate security methods
- Evaluate an optimal mix of network design and operational parameters to ensure network scalability and throughput
- Evaluate the trade-off between security and computational complexity

Sample Projects

- Project 1: Independently research a current blockchain application and analyze its viability
- Project 2: Determine validity of Merkle proofs
- Project 3: Verify signatures with software
- Project 4: Build a blockchain

Course Content

Instruction

- Video lectures
- Other videos
- Readings
- Interactive learning objects
- Live office hours

Assessments

- Practice activities and quizzes (auto-graded)
- Practice assignments (instructor- or peer-reviewed)
- Team and/or individual project(s) (instructor-graded)
- Midterm and final exam (proctored, graded)

Estimated Workload/ Time Commitment Per Week

Approximately 15-20 hours per week.

Technology Requirements

Hardware

- Standard with major OS

Software and Other

- Standard - technology integrations will be provided through Coursera

Course Outline

Unit 1: The Blockchain's Abstractions and Applications

Learning Objectives

1.1 Describe the basic blockchain data structure
1.2 Describe key benefits of blockchain technology
1.3 Identify an industry that can be improved with the benefits of blockchain
1.4 Describe applications of blockchain technology
1.5 Analyze the viability of a current blockchain application
1.6 Describe the blockchain ecosystem as a whole

Module 1: Introduction to Blockchain Technology

Unit Introduction
Blockchain Technology through an Analogy
Accompanying Factors

Module 2: Benefits of Blockchain Technology

Transparency
Traceability
Security
Immutability
Availability
Cost-Saving

Module 3: Blockchain Applications

Currency/Payments
Smart Contracts
Supply Chain
Governance
File Storage
Internet of Things (IoT)
Identity Management
Data Management
Land Title Registration
Stock Trading

Module 4: The Blockchain Ecosystem

Financial Services
General Business
UX/UI Design
Legal
Education

Unit 2: Hash Functions with Applications

Learning Objectives

2.1 Recognize possible malware by comparing the hashes of software packages
2.2 Identify proper password handling practices
2.3 Estimate expected time required for brute forcing a collision of secure hash functions
2.4 Evaluate the validity of a Merkle proof as applied to SPV wallets

Module 1: Introduction to Hash Functions

Definition
Evaluating Security of a Hash Function
Side Channel Attacks w/ Mitigation
Examples of Hash functions

- MD5 (depreciated)
- SHA1 (deprecated)
- SHA256
- RPEMD-160
- SHA256
- PBKDF2 (Password Based Key Derivation Function 2)

Module 2: Password Handling

Problems with storing passwords in plain text

- Access granted to anyone maintaining the database
- One database breach will divulge passwords

Rainbow table attack
Appropriately salted hashes
Use of Pepper

Module 3: Application Appropriate Hash Function

Fast hash function
Slow hash function
Memory Hard

Module 4: Merkel Trees

Construction/Definition
Merkel Root
A Merkel Proof
Application to SPV

Unit 3: Cryptography and Mathematical Foundations for Blockchains

Learning Objectives

3.1 Perform calculations with finite fields
3.2 Identify the sum of two points on a picture of an elliptic curve
3.3 Use computer software to convert from a number to the compressed form of a point on secp256k1
3.4 Use computer software to determine if a signature (of a hash of the message) is valid or invalid
3.5 Identify side-channel attacks in the context of cryptography.

Module 1: Signatures

- Elliptic Curves (background for ECDSA)
- Public/Private Keys (ECDSA)
- Verifying signatures with software

Module 2: Storage Considerations

- Binomial Distribution
- Stable Nash Equilibrium
- Cold and Warm storage of private keys
- Address format

Unit 4: Programming abstractions for the blockchain

Learning Objectives

4.1 Interpret and Evaluate Dash scripts written in Reverse Polish Notation
4.2 Write a script to hash locking script/multisig
4.3 Identify proper salting of hash functions
4.4 Identify for what applications cryptographic tools (Merkle Tree, Bloom Filter, etc.) are used
4.5 Identify how each block updates the UTXO
4.6 Write locking and unlocking script (P2PKH)

Module 1: Transactions

Module 2: Scripts

Module 3: State Channels

Module 4: Wallets

Unit 5: Blockchain Consensus

Learning Objectives

5.1 Distinguish among the three types of blockchain consensus
5.2 Illustrate consensus algorithms and what miners do in each

Module 1: Permissionless

Proof of work
Proof of stake
Distributed Proof of Stake
Hybrid

Module 2: Permissioned

Probabilistic agreement
Paxos and variants
Honey badger and similar

Module 3: Semi-permissioned

Ripple

Unit 6: Mining

Learning Objectives

6.1 Calculate the future difficulty rate given the current block rate and the target rate
6.2 Verify that work done on a given chain is sufficient
6.3 Explain different Incentives/Strategies miners have
6.4 Identify the role of mining pools in the network
6.5 Differentiate among the different types of mining nodes

Module 1: Network Architecture

Nakamoto Networks
Blockchain Architecture

- Blocks form a chain
- "Longest" (most work) chain is considered correct

Module 2: Network Attacks

Difficulty of a 51% attack
Selfish miner attack
Deriving the Global State or UTXO from a block chain
Consensus as a tool

Unit 7: Peer-to-peer networks

Learning Objectives

7.1: Identify the different node types in a cryptocurrency/blockchain network
7.2: Describe how nodes discover the network (other peers)
7.3: Describe how nodes, once connected, choose a blockchain history and receive the historical data
7.4: Describe how transactions/messages are verified and propagated throughout the network
7.5: Describe how blocks are verified and propagated throughout the network
7.6: Illustrate how SPV (Simplified Payment Verification) clients work and interact with the network

Module 1: Introduction to Network Topology

Closed systems
Decentralized networks
Identification and interaction of nodes

Module 2: Nodes

Basic concepts
Valid and invalid blocks
Roles and behaviors in hierarchical networks

Module 3: Block Verification and Propagation

Signal process
Signal outcomes
BIP 9, block version signaling consensus change
Fee amount
Contentious forks/minority forks

Unit 8: Governance

Learning Objectives

8.1: Describe how decisions are made on a decentralized network (understanding BIP, DIP, EIP generalized processes)
8.2: Identify the updates that would result in a chain fork
8.3: Illustrate the process of signaling to a network using BIP 9 code to run through a simulated blockchain that tracks the signal and the outcome
8.4: Describe contentious forks/minority forks
8.5: Create a timeline for a successful hard fork

Module 1: Decision-Making on Decentralized Networks

BIP
DIP
EIP generalized processes

Module 2: Hard and Soft Forks

Hard forks
Soft forks
Updating to achieve hard forks

About ASU

Established in Tempe in 1885, Arizona State University (ASU) has developed a new model for the American Research University, creating an institution that is committed to access, excellence and impact.

As the prototype for a New American University, ASU pursues research that contributes to the public good, and ASU assumes major responsibility for the economic, social and cultural vitality of the communities that surround it. Recognizing the university's groundbreaking initiatives, partnerships, programs and research, U.S. News and World Report has named ASU as the most innovative university all three years it has had the category.

The innovation ranking is due at least in part to a more than 80 percent improvement in ASU's graduation rate in the past 15 years, the fact that ASU is the fastest-growing research university in the country and the emphasis on inclusion and student success that has led to more than 50 percent of the school's in-state freshman coming from minority backgrounds.

About Ira A. Fulton Schools of Engineering

Structured around grand challenges and improving the quality of life on a global scale, the Ira A. Fulton Schools of Engineering at Arizona State University integrates traditionally separate disciplines and supports collaborative research in the multidisciplinary areas of biological and health systems; sustainable engineering and the built environment; matter, transport and energy; and computing and decision systems. As the largest engineering program in the United States, students can pursue their educational and career goals through 25 undergraduate degrees or 39 graduate programs and rich experiential education offerings. The Fulton Schools are dedicated to engineering programs that combine a strong core foundation with top faculty and a reputation for graduating students who are aggressively recruited by top companies or become superior candidates for graduate studies in medicine, law, engineering and science.

About the School of Computing, Informatics, & Decision Systems Engineering

The School of Computing, Informatics, and Decision Systems Engineering advances developments and innovation in artificial intelligence, big data, cybersecurity and digital forensics, and software engineering. Our faculty are winning prestigious honors in professional societies, resulting in leadership of renowned research centers in homeland security operational efficiency, data engineering, and cybersecurity and digital forensics. The school's rapid growth of student enrollment isn't limited to the number of students at ASU's Tempe and Polytechnic campuses as it continues to lead in online education. In addition to the Online Master of Computer Science, the school also offers an Online Bachelor of Science in Software Engineering, and the first four-year, completely online Bachelor of Science in Engineering program in engineering management.

Creators

Dragan Boscovic is a research professor in the School of Computing, Informatics, & Decision Systems Engineering (CIDSE), as well as Technical Director of CIDSE's Center for Assured and Scalable Data Engineering and Distinguished Visiting Scholar, mediaX, at Stanford University. Dr. Boscovic also leads ASU's Blockchain Research Lab, where his team's mission is to advance the research and development of blockchain-based technologies for use in business, finance, economics, mathematics, computer science, and all other areas of potential impact.

He holds a Ph.D. in EE and CS, Numerical Electromagnetic Modeling from University of Bath, United Kingdom (1991) and a Magistar in EE, eq. Ph.D., Microwave and Optoelectronics from University of Belgrade, Serbia (1988). He has 25 years of high tech experience acquired in an international set up (i.e. UK, France, China, USA) and is uniquely positioned to help data-driven technical advances within today's global data-intensive technology arena. He is a lateral thinker with broad exposure to a wide range of scientific methods and business practices and has a proven track record in conceiving strategies and managing development, investment and innovation efforts as related to advanced data analysis services, user experience, and mobile and IoT solutions and platforms.

Darren Tapp was involved in the development of Bitcoin and is now a researcher on the digital cash (cryptocurrency) development team at dash.org, a non-profit blockchain technology startup. He earned his doctorate in mathematics from Purdue University in 2007 and holds both a bachelor's degree in physics and mathematics and a master's degree in mathematics from the University of Kentucky. Most recently he has taught both on-ground and online at schools including Southern New Hampshire University, NHTI - Concord's Community College, and Hesser College. He lives in New Hampshire, where he volunteers promoting STEM subjects to high-school-aged members of the Big Fish Learning Community.