BLENDED DELIVERY - ON-DEMAND & LIVE INSTRUCTOR LED ONLINE

SYLLABUS

BLOCKCHAIN SECURITY COURSE

Duration: 20 Hours

Delivery: Online On-Demand

Instructor(s): Howard Poston & Jim Sullivan

Office Hours: 10:00 AM to 6:00 PM Eastern Standard Time

Email: studentsupport@theblockchainacademy.com

Prerequisites: None

Microcredential Exam: Blockchain Security Microcredential
Certification Body: Blockchain Certification Association (BCA)

Course Overview:
The Blockchain Security Course will provide an in-depth introduction to the security risks of blockchain platforms and how to remediate them. Course attendees will explore blockchain security from the fundamental principles up through the smart contracts that run on top of the platform.

Course Composition:

Online On-Demand:	Blockchain Security	Modules 1 - 13
LIVE Instrucotr Led Online	Blockchain Security Workshop	
LIVE Instrucotr Led Online	Ask Me Anything - Weekly Session	

Learning Objectives:

- Understand the security of blockchain's fundamental cryptography.
- Explore the advantages and disadvantages of blockchain consensus algorithms.
- Identify the security impacts of blockchain infrastructure, such as nodes and networks.
- Discuss the security of smart contracts and their applications.
- Define how to develop a secure blockchain-based solution for a business case.

Demonstration of Learning Outcomes:
After the Smart Contract Security Course, students understand common smart contract vulnerabilities and how to identify and correct them.

Evaluation:
Evaluation is based on participation and a final exam.
Weighted:

50% participation
50% on the final grade

80% overall grade is required to receive a Certificate of Completion.

Grading Policy:
Pass or Fail. No Credit (NC).

Attendance Requirements:
Students are expected to complete all online self-paced modules and assessments. Certificate of Completion will not be issued until all online modules are complete, including the final exam.

Student conduct and etiquette:
Students will be expected to be courteous in their conduct and communications to the instructor and classmates at all times, whether such conduct or communication is in person, by telephone, or electronic communications.

Behavior that persistently or grossly interferes with the instructor or other student activities is considered disruptive behavior and may be subject to disciplinary action. Such behavior inhibits other students' ability to learn, and an instructor's ability to teach. The instructor may require a student responsible for disruptive behavior to leave the learning environment pending discussion and resolution of the problem and may report a disruptive student to the Student Affairs Office.

Note: Disruptions or any other distraction in the learning environment may result in a failing grade.

Course Evaluations
Course evaluations and program surveys are important components of the educational process. Students are encouraged to complete the student course evaluation form issued after the course. The review is anonymous.

Computer/Information Literacy Expectations for Students enrolled in this class.
Students in this class are expected to:

1. Use a word processing program for writing assignments (e.g., Microsoft Word)
2. Be able to access assigned websites through the internet.
3. Have access to PC or mobile device for participation in course content

Course Module Overview:

SMART CONTRACT SECURITY COURSE – 6 MODULES

Module 1: Introduction to Blockchain Security
Introduction to the Blockchain
How the Blockchain Works
Core Features of Blockchain Technology

Module 2: Cryptography in the Blockchain
Introduction to Blockchain Cryptography
Hash Functions
Public Key Cryptography
Case Study: Lisk

Module 3: Blockchain Consensus
Introduction to Consensus
Proof of Work Security
Proof of Stake Security
Case Study: Verge

Module 4: Advanced Blockchain Security Mechanisms
Introduction to Advanced Security
Architectural Security
Advanced Cryptographic Tools

Module 5: Blockchain User and Node Security
Introduction to User and Node Security
Securing the Blockchain User
Securing the Blockchain Node
Case Study: Ethereum RPC

Module 6: Securing the Blockchain Network
The Blockchain Peer-to-Peer Network
Attacking the Blockchain Network
Denial of Service Attacks
Eclipse/Routing Attacks
Sybil Attacks

Module 7: Introduction to Smart Contract Security
Introduction to Smart Contracts
Smart Contract Security and Vulnerabilities

Module 8: General Programming Vulnerabilities
What Are General Programming Vulnerabilities?
Arithmetic Vulnerabilities

External Library Functions
Right-to-Left Control Characters

Module 9: Blockchain-Specific Vulnerabilities
What are Blockchain-Specific Vulnerabilities?
Access Control
Denial of Service
Frontrunning
Rollback Attacks
Timestamp Dependence
Weak Randomness

Module 10: Ethereum-Specific Vulnerabilities
Introduction to Common Ethereum Mistakes
Denial of Service: Block Gas Limits
Denial of Service: Unexpected Revert
Forced Send of Ether
Reentrancy
Short Addresses
Unchecked Return Values
Unsafe External Calls

Module 11: Decentralized Finance (DeFi) Vulnerabilities
Introduction to DeFi Vulnerabilities
Access Control
Control and Governance Issues
Frontend Vulnerabilities
Price Manipulation

Module 12: Smart Contract Security Best Practices
Secure Smart Contract Development
Secure Smart Contract Auditing

Module 13: Developing Secure Blockchain Solutions for Business
Designing Blockchain Solutions
Assessing Blockchain Use Cases
Blockchain and Compliance