BLOCKCHAIN SECURITY TRAINING

Course Outline:

Fundamental Blockchain Security

• Cryptography for the Blockchain

• A Brief Introduction to Blockchain

• Blockchain Security Assumptions

• Limitations of Basic Blockchain Security

Consensus in the Blockchain

• Blockchain Consensus and Byzantine Generals

• Introduction to Blockchain Consensus Security

◦ Proof of Work

◦ Proof of Stake

◦ Other Blockchain Consensus Algorithms

Advanced Blockchain Security Mechanisms

• Architectural Security Measures

◦ Permissioned Blockchains

◦ Checkpointing

• Advanced Cryptographic Solutions

◦ Multiparty Signatures

◦ Zero-Knowledge Proofs

◦ Stealth Addresses

◦ Ring Signatures

◦ Confidential Transactions

Smart Contract Security

• Introduction to Smart Contracts

• Smart Contract Security Considerations

• Smart Contract Code Auditing

Blockchain Risk Assessment

• Blockchain Risk Considerations

• Regulatory Requirements

• Blockchain Architectural Design

Basic Blockchain Security

• User Security

• Node Security

• Network Security

Blockchain for Business

• Introduction to Ethereum Security

• Introduction to Hyperledger Security

• Introduction to Corda Security

Securely Implementing Business Blockchains

• Business Operations

• Data Management

• Infrastructure

• Legal and Regulatory Compliance

Network-Level Vulnerabilities and Attacks

• 51% Attacks

• Denial of Service Attacks

• Eclipse Attacks

• Replay Attacks

• Routing Attacks

• Sybil Attacks

System-Level Vulnerabilities and Attacks

• The Bitcoin Hack

• The Verge Hack

• The EOS Vulnerability

• The Lisk Vulnerability

Smart Contract Vulnerabilities and Attacks

• Reentrancy

• Access Control

• Arithmetic

• Unchecked Return Values

- Denial of Service
- Bad Randomness
- Race Conditions
- Timestamp Dependence
- Short Addresses

Security of Alternative DLT Architectures

- Introduction to DAG-Based DLTs
- Advantages of DAG-Based DLTs
- Limitations of DAG-Based DLTs