Blockchain Security Training

Category: Networking & Security | **Vendor:** Blockchain Training Alliance

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course covers all known aspects of Blockchain security that exist in the Blockchain environment today and provides a detailed overview of all Blockchain security issues, including threats, risk mitigation, node security integrity, confidentiality, best security practices, advanced Blockchain security and more.

About This Course

This course covers all known aspects of Blockchain security that exist in the Blockchain environment today and provides a detailed overview of all Blockchain security issues, including threats, risk mitigation, node security integrity, confidentiality, best security practices, advanced Blockchain security and more.

Who Should Attend

Blockchain Architects Blockchain DevelopersApplication Developers Blockchain System AdministratorsNetwork Security Architects Cyber Security ExpertsIT Professionals w/cyber security experience

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Those who attend the Security for Blockchain Professionals course and pass the exam certification will have a demonstrated knowledge of:Identifying and differentiating between security threats and attacks on a Blockchain network.Blockchain security methods, best practices, risk mitigation, and more.All known (to date) cyber-attack vectors on the Blockchain.Performing Blockchain network security risk analysis.A complete understanding of Blockchain's inherent security features and risks.An excellent knowledge of best security practices for Blockchain System/Network Administrators.Demonstrating appropriate Blockchain data safeguarding techniques.

Detailed Course Outline

Fundamental Blockchain Security Cryptography for the Blockchain Hash Functions

- Public Key Cryptography
- Elliptic Curve Cryptography
- A Brief Introduction to Blockchain The Blocks
- The Chains
- The Network
- Promises of the Blockchain
- Blockchain Security Assumptions Digital Signature Security
- Hash Function Security
- Limitations of Basic Blockchain Security Public Key Cryptography Review
- Real-Life Public Key Protection
- Cryptography and Quantum Computers
- Lab 1 (Tentative) Finding Hash Function Collisions Reversible hash function
- Hash function with poor non-locality
- Hash function with small search space
- Breaking Public Key Cryptography Brute Forcing a Short Private Key
- Brute Forcing a Poorly-Chosen Private Key

Consensus in the Blockchain

- Blockchain Consensus and Byzantine Generals Blockchain Networking Review
- Byzantine Generals Problem Relation to Blockchain
- Byzantine Fault Tolerance
- Introduction to Blockchain Consensus Security Blockchain Consensus Breakthrough
- Proof of Work What is Proof of Work
- How does Proof of Work Solve BGP
- Proof of Work Security Assumptions
- Attacking Proof of Work
- Proof of Stake What is Proof of Stake
- How does Proof of Stake Solve BGP
- Proof of Stake Security Assumptions
- Attacking Proof of Stake
- General Attacks on Blockchain Consensus
- Other Blockchain Consensus Algorithms
- Lab 2 (Tentative) Attacking Proof of Work Performing a 51% Attack
- Performing a Selfish Mining Attack
- Attacking Proof of Stake Performing a XX% Attack
- Performing a Long-Range Attack
- Malleable Transaction Attacks

Advanced Blockchain Security Mechanisms Architectural Security Measures Permissioned Blockchains

- Checkpointing
- Advanced Cryptographic Solutions Multiparty Signatures
- Zero-Knowledge Proofs
- Stealth Addresses
- Ring Signatures
- Confidential Transactions
- Lab 3 (Tentative) Permissioned Blockchains
- 51% on a Checkpointed Blockchain
- Data mining on a blockchain with/without stealth addresses
- Zero-Knowledge Proof Simulation
- Trying to fake knowledge of a ZKP
- Module 4: Blockchain for Business Introduction to Ethereum Security What is Ethereum
- Consensus in Ethereum
- Smart Contracts in Ethereum
- Ethereum Security
- Pros and Cons of Ethereum Blockchains
- Introduction to Hyperledger Security What is Hyperledger
- Consensus in Hyperledger
- Smart Contracts in Hyperledger
- Hyperledger Security
- Pros and Cons of Hyperledger Blockchains
- Introduction to Corda Security What is Corda
- Consensus in Corda
- Smart Contracts in Corda
- Corda Security
- Pros and Cons of Corda Blockchains
- Lab 4

Blockchain Risk Assessment What are the Risks of the Blockchain

- Information Security
- Information Sensitivity Data being placed on blockchain
- Risks of disclosure
- Regulatory Requirements Data encryption
- Data control
- PII protection
- Blockchain Architectural Design Public and Private Blockchains
- Open and Permissioned Blockchains
- Choosing a Blockchain Architecture
- Lab 5
- Exploring public/private open/permissioned blockchains

Basic Blockchain Security Blockchain Architecture

- User Security Protecting Private Keys
- Malware
- Update
- Node Security
- Configuring MSPs
- Network Security
- Lab 6 (TBD)

Smart Contract Security Introduction to Smart Contracts

- Smart Contract Security Considerations Turing-Complete
- Lifetime
- External Software
- Smart Contract Code Auditing Difficulties
- Techniques
- Tools
- Lab 7 (Tentative)
- Try a couple of smart contract code auditing tool against different contracts with built-in vulnerabilities
- Module 8: Security Implementing Business Blockchains Ethereum Best Practices
- Hyperledger Best Practices
- Corda Best Practices
- Lab 8

Network-Level Vulnerabilities and Attacks Introduction to Blockchain Network Attacks

- 51% Attacks
- Denial of Service Attacks
- Eclipse Attacks
- Routing Attacks
- Sybil Attacks
- Lab 9
- Perform different network-level attacks

System-Level Vulnerabilities and Attacks Introduction to Blockchain System Vulnerabilities

- The Bitcoin Hack
- The Verge Hack
- The EOS Vulnerability
- Lab 10

Smart Contract Vulnerabilities and Attacks Introduction to Common Smart Contract Vulnerabilities

- Reentrancy
- Access Control
- Arithmetic
- Unchecked Return Values
- Denial of Service
- Bad Randomness
- Race Conditions
- Timestamp Dependence
- Short Addresses
- Lab 11
- Exploiting vulnerable smart contracts

Security of Alternative DLT Architectures What Are Alternative DLT Architectures

- Introduction to Directed Acyclic Graphs (DAGs)
- DAGs vs. Blockchains
- Advantages of DAGs
- DAG Vulnerabilities and Security
- Lab 12
- Exploring a DAG network

Additional Course Details

Nexus Humans Blockchain Security Training training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the Blockchain Security Training course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for Blockchain Security Training?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Blockchain Security Training course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Blockchain Security Training training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Blockchain Security Training?

Yes, we provide corporate training, dedicated training, and closed classes for Blockchain Security Training. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for Blockchain Security Training?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Blockchain Security Training training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.