Blockchain Security and Cryptocurrency Fundamentals Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapidly evolving landscape of Web3 and Decentralized Finance (DeFi) has brought Blockchain Technology from a niche concept to a global economic force, fundamentally reshaping industries from finance to supply chain management. While the inherent features of immutability and decentralization make blockchain a powerful, trustless system, its complexity introduces unique and significant cybersecurity challenges. This requires a new generation of expertise capable of navigating the vulnerabilities of smart contracts, safeguarding cryptocurrency assets against sophisticated attacks like 51% attacks and reentrancy flaws, and ensuring full regulatory compliance. Understanding the cryptographic underpinnings from hashing to public-key infrastructure is no longer optional; it is the core competency needed to protect the trillion-dollar digital asset ecosystem and build secure DApps.

Blockchain Security and Cryptocurrency Fundamentals Training Course is designed to bridge the gap between foundational cryptocurrency fundamentals and advanced blockchain security architecture. Participants will gain the practical knowledge to identify, analyze, and mitigate threats across the entire decentralized technology stack, encompassing layer-1 protocols, wallets, and decentralized exchanges. We emphasize risk assessment, vulnerability testing, and the implementation of security-by-design principles for developing and deploying robust DLT solutions. By mastering topics like consensus mechanisms, tokenomics, and zero-knowledge proofs, learners will emerge as certified experts ready to lead digital asset protection strategies in any forward-thinking organization.

Programme Curriculum

Blockchain Security and Cryptocurrency Fundamentals Training Course

Introduction

The rapidly evolving landscape of Web3 and Decentralized Finance (DeFi) has brought Blockchain Technology from a niche concept to a global economic force, fundamentally reshaping industries from finance to supply chain management. While the inherent features of immutability and decentralization make blockchain a powerful, trustless system, its complexity introduces unique and significant cybersecurity challenges. This requires a new generation of expertise capable of navigating the vulnerabilities of smart contracts, safeguarding cryptocurrency assets against sophisticated attacks like 51% attacks and reentrancy flaws, and ensuring full regulatory compliance. Understanding the cryptographic underpinnings from hashing to public-key infrastructure is no longer optional; it is the core competency needed to protect the trillion-dollar digital asset ecosystem and build secure DApps.

Blockchain Security and Cryptocurrency Fundamentals Training Course is designed to bridge the gap between foundational cryptocurrency fundamentals and advanced blockchain security architecture. Participants will gain the practical knowledge to identify, analyze, and mitigate threats across the entire decentralized technology stack, encompassing layer-1 protocols, wallets, and decentralized exchanges. We emphasize risk assessment, vulnerability testing, and the implementation of security-by-design principles for developing and deploying robust DLT solutions. By mastering topics like consensus mechanisms, tokenomics, and zero-knowledge proofs, learners will emerge as certified experts ready to lead digital asset protection strategies in any forward-thinking organization.

Course Duration

5 days

Course Objectives

1. Master the fundamental Cryptography principles underpinning Blockchain and Cryptocurrency transactions.
2. Analyze and differentiate between various Consensus Mechanisms and their respective security risks.
3. Perform comprehensive Smart Contract Auditing to identify and mitigate critical vulnerabilities like Reentrancy and Overflow.
4. Design and implement Secure DApps using best practices for popular platforms like Ethereum and Hyperledger.
5. Evaluate the threat landscape, including 51% Attacks, Sybil Attacks, and other network-level exploits on DLTs.
6. Secure Digital Wallets and manage Private Keys using robust Key Management strategies.
7. Understand the principles of Decentralized Finance Security and risks associated with Yield Farming and Liquidity Pools.
8. Implement Zero-Knowledge Proofs and other Privacy-Enhancing Technologies for data confidentiality.
9. Navigate the complex global regulatory environment, including AML/KYC for Digital Assets and Travel Rule compliance.
10. Develop an effective Blockchain Forensics and Incident Response Plan for tracing and recovering stolen crypto-assets.
11. Assess the impact of emerging threats like Quantum Computing on current Blockchain Cryptography standards.
12. Explore the security implications of Tokenization of Real-World Assets and NFT platforms.
13. Apply Blockchain Risk Assessment frameworks to enterprise-level Supply Chain and Identity Management solutions.

Target Audience

1. Blockchain Developers and Software Engineers building DApps and Smart Contracts.
2. Cybersecurity Professionals and Security Analysts
3. FinTech Specialists and Financial Auditors.
4. System/Network Administrators.
5. Chief Information Security Officers and IT Managers.
6. Compliance Officers and Legal Professionals.
7. Venture Capitalists and Investors.
8. Enterprise Architects evaluating Permissioned and Consortium Blockchain solutions

Course Modules

Module 1: Cryptography and Blockchain Fundamentals

- The Power of Hashing.
- Public-Key Cryptography.
- Blockchain Architecture.
- Transaction Lifecycle.
- Case Study: Analyzing the failure of centralized key management and the need for secure, decentralized alternatives.

Module 2: Consensus Mechanisms and Network Security

- Deep dive into mining, difficulty adjustments, and the cost of 51% Attacks.
- Exploring staking, finality, and the different security models of PoS
- Network-Level Attacks.
- Node Integrity.
- Case Study: Examining how a less secure network was successfully exploited by concentrated hashing power.

Module 3: Smart Contract Vulnerabilities and Secure Coding

- Detailed analysis of Reentrancy, Integer Overflow/Underflow, and Timestamp Dependence.
- Implementing best practices for secure Smart Contract Development and code logic.
- Proper use of Modifiers and the onlyOwner pattern to prevent unauthorized state changes.
- Testing and Auditing Tools.
- Case Study: Dissecting the reentrancy flaw that led to one of the largest early exploits and the subsequent Ethereum hard fork.

Module 4: Wallet Security and Key Management

- Differentiating between Hot (online), Cold (offline), Hardware, and Multisignature wallets.
- Seed Phrase/Mnemonic Security.
- Advanced Key Management.
- Understanding how Hierarchical Deterministic (HD) Wallets derive keys.
- Case Study: LastPass Breach and other major platform compromises, emphasizing that the custodian is often the weakest link in the security chain.

Module 5: Decentralized Finance (DeFi) Security

- DeFi Attack Vectors.
- Assessing the risk of Impermenent Loss and economic exploits in lending and borrowing protocols.
- Securing Bridges and Cross-Chain Communication.

- Decentralized Autonomous Organizations.
- Case Study: Investigating the signature verification flaw that resulted in a massive loss of funds.

Module 6: Regulatory Compliance and Blockchain Forensics

- Implementing regulatory requirements for exchanges and centralized financial service providers.
- Utilizing Blockchain Analytics tools to track illicit funds and perform Chain Hopping analysis.
- Overview of global regulations like MiCA and US SEC guidance on Digital Assets.
- Balancing transparency with privacy using techniques like Zero-Knowledge Proofs
- Case Study: Tracing the Bitcoin payment and subsequent seizure by law enforcement using Blockchain Forensics.

Module 7: Enterprise and Advanced DLT Security

- Permissioned DLT Security.
- Tokenization Security.
- Supply Chain Security.
- Decentralized Identity.
- Case Study: The Maersk/IBM TradeLens platform security architecture how a consortium blockchain ensures trust and immutability across competing partners.

Module 8: Emerging Threats and Future-Proofing

- Introduction to Post-Quantum Cryptography and the looming threat to current PKI.
- Understanding the security trade-offs and vulnerabilities in Rollups and State Channels.
- AI and Blockchain.
- Security Audits and Bug Bounties.
- Case Study: Analyzing the technical and governance failures that led to network halt and the importance of stress testing and high availability.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org **or call** +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com