Training Course on Smart Contracts and Decentralized Application Forensics

Professional Development Training Course Outline

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

Course Introduction

The burgeoning landscape of **blockchain technology** has ushered in an era of **decentralized applications (DApps)** and **self-executing smart contracts**, revolutionizing industries from finance to supply chain. While these innovations promise unparalleled efficiency and transparency, they also introduce complex **cybersecurity challenges** and novel **forensic investigation** needs. As the value locked in decentralized finance (DeFi) protocols and the volume of on-chain transactions skyrocket, the imperative for specialized expertise in **Smart Contract and DApp Forensics** becomes paramount to mitigate risks, ensure compliance, and effectively respond to security incidents.

Training Course on Smart Contracts and Decentralized Application Forensics provides a comprehensive deep dive into the **forensic analysis** of **smart contracts** and **decentralized applications**. Participants will gain critical skills to identify, analyze, and investigate **on-chain anomalies**, **exploit vulnerabilities**, and **recover digital assets** in the wake of **blockchain security breaches**. Through practical methodologies and real-world **case studies**, this program empowers professionals to navigate the intricate world of **Web3 investigations** and safeguard the integrity of decentralized ecosystems.

Programme Curriculum

Training Course on Smart Contracts and Decentralized Application Forensics

Introduction

The burgeoning landscape of **blockchain technology** has ushered in an era of **decentralized applications (DApps)** and **self-executing smart contracts**, revolutionizing industries from finance to supply chain. While these innovations promise unparalleled efficiency and transparency, they also introduce complex **cybersecurity challenges** and novel **forensic investigation** needs. As the

value locked in decentralized finance (DeFi) protocols and the volume of on-chain transactions skyrocket, the imperative for specialized expertise in **Smart Contract and DApp Forensics** becomes paramount to mitigate risks, ensure compliance, and effectively respond to security incidents.

Training Course on Smart Contracts and Decentralized Application Forensics provides a comprehensive deep dive into the **forensic analysis** of **smart contracts** and **decentralized applications**. Participants will gain critical skills to identify, analyze, and investigate **on-chain anomalies**, **exploit vulnerabilities**, and **recover digital assets** in the wake of **blockchain security breaches**. Through practical methodologies and real-world **case studies**, this program empowers professionals to navigate the intricate world of **Web3 investigations** and safeguard the integrity of decentralized ecosystems.

Course Duration

5 days

Course Objectives

1. Develop a foundational understanding of **blockchain architecture**, **cryptographic principles**, and **transaction immutability** relevant to forensic investigations.
2. Identify and comprehend common **smart contract exploit vectors** including **reentrancy**, **integer overflow/underflow**, **access control flaws**, and **front-running attacks**.
3. Learn advanced techniques for **cryptocurrency tracing**, **fund flow analysis**, and identifying illicit activities across various **blockchain networks**.
4. Acquire methodologies for responding to and investigating **decentralized application hacks**, including **DeFi exploits** and **NFT rug pulls**.
5. Gain proficiency in using cutting-edge **blockchain forensics platforms** and **on-chain analysis tools** for data extraction and visualization.
6. Develop skills in reviewing and auditing **Solidity smart contract code** for security weaknesses and compliance issues.
7. Understand the mechanics of **oracle manipulation** and its impact on DApps, along with techniques for forensic detection.
8. Explore strategies and legal considerations for **recovering stolen digital assets** and funds from compromised smart contracts or DApps.
9. Analyze the security risks associated with **cross-chain bridges** and methodologies for investigating multi-chain incidents.
10. Evaluate the vulnerabilities inherent in **DAO governance models** and their potential for exploitation in decentralized ecosystems.
11. Formulate effective **Web3 incident response plans** tailored to blockchain and DApp security breaches.
12. Understand the evolving **legal landscape** surrounding **digital asset investigations**, **cybercrime**, and **AML/CFT compliance** in the blockchain space.
13. Learn to compile comprehensive and admissible **blockchain forensic reports** for legal proceedings and internal investigations.

Organizational Benefits

- Strengthen capabilities to proactively identify and mitigate **smart contract risks** and **DApp vulnerabilities**, reducing the likelihood of costly security breaches.
- Develop in-house expertise to effectively respond to and **investigate blockchain security incidents**, minimizing financial losses and reputational damage.

- Equip teams with the knowledge to navigate complex **AML (Anti-Money Laundering)**, **CFT (Combating the Financing of Terrorism)**, and data privacy regulations in the context of **decentralized finance**.
- Protect organizational and client **digital assets** by understanding advanced **forensic techniques** for **fund tracing** and **recovery**.
- Demonstrate a commitment to **blockchain security** and **responsible DApp development**, fostering trust among users, investors, and partners.
- Mitigate financial risks associated with **smart contract exploits**, **DeFi hacks**, and other **cybercrime activities** in the Web3 space.
- Enable secure experimentation and deployment of **blockchain solutions** by integrating **forensic best practices** into the development lifecycle.

Target Audience

1. Cybersecurity Professionals.
2. Digital Forensic Investigators.
3. Blockchain Developers & Auditors.
4. Law Enforcement & Government Agencies.
5. Financial Crimes Investigators.
6. Risk Management Professionals
7. Legal Professionals
8. Compliance Officers.

Course Outline

Module 1: Introduction to Blockchain & Smart Contract Foundations

- Fundamentals of Blockchain Technology.
- Understanding Smart Contracts
- Decentralized Applications (DApps
- Introduction to Blockchain Forensics
- Legal & Ethical Considerations
- **Case Study: Bitcoin's Pseudonymity**: Analyzing the early days of Bitcoin and how initial assumptions about anonymity were challenged by forensic techniques.

Module 2: Smart Contract Vulnerabilities & Attack Vectors

- Common Solidity Vulnerabilities.
- Economic Exploits
- Front-Running & MEV (Maximal Extractable Value).
- Denial-of-Service (DoS) Attacks.
- Logic Bugs & Design Flaws.
- **Case Study: The DAO Hack (2016)**: Deep dive into the infamous reentrancy attack that led to a hard fork of Ethereum, highlighting vulnerability identification and response.

Module 3: On-Chain Data Acquisition & Analysis

- Blockchain Explorers
- Node Interaction
- Decoding Transaction Data.
- Smart Contract Disassembly & Decompilation.
- Data Visualization & Clustering

- **Case Study: Bitfinex Hack (2016)**: Tracing the movement of stolen Bitcoin through multiple addresses and exchanges using on-chain analytics.

Module 4: Cryptocurrency Tracing & Fund Flow Analysis

- Wallet Forensics.
- Exchange Analysis
- Mixers & Tumblers
- Cross-Chain Transactions.
- Automated Tracing Tools
- **Case Study: Colonial Pipeline Ransomware (2021)**: Forensic tracing of Bitcoin ransom payments and subsequent recovery efforts.

Module 5: Decentralized Application (DApp) Forensics

- DeFi Protocol Investigations
- NFT Frauds & Rug Pulls.
- DAO Governance Exploits
- Front-End & DNS Hijacking.
- Interacting with Compromised DApps
- **Case Study: Poly Network Hack (2021)**: Analyzing the largest DeFi exploit to date, focusing on **cross-chain bridge vulnerabilities** and the subsequent negotiation for fund return.

Module 6: Smart Contract Code Auditing & Static Analysis

- Introduction to Smart Contract Auditing
- Automated Static Analysis Tools
- Manual Code Review Techniques
- Gas Optimization & Efficiency.
- Upgradeability & Proxy Contracts.
- **Case Study: Parity Multisig Wallet Freeze (2017)**: Analyzing the vulnerability in the Parity wallet that allowed an attacker to "kill" the contract, rendering funds inaccessible.

Module 7: Digital Asset Recovery & Legal Aspects

- Strategies for Fund Recovery
- Freezing Stolen Assets.
- Jurisdictional Challenges
- Chain of Custody for Digital Evidence.
- Expert Witness Testimony.
- **Case Study: Ronin Bridge Hack (2022)**: Exploring the efforts to recover over $600 million in stolen cryptocurrency, highlighting international collaboration and asset tracing complexities.

Module 8: Advanced Topics & Future Trends in Blockchain Forensics

- Privacy Coins & ZK-Proofs
- Layer 2 Solutions & Sidechains.
- Decentralized Storage Forensics (IPFS, Arweave)
- AI/ML in Blockchain Forensics
- Regulatory Evolution & Compliance Frameworks.

- **Case Study: Tornado Cash Sanctions (2022)**: Discussing the impact of government sanctions on a decentralized mixing service and the forensic challenges it presents.

Training Methodology

This course employs a **blended learning approach** designed for maximum engagement and practical skill acquisition:

- **Interactive Lectures**: Concise presentations of core concepts, theories, and methodologies.
- **Hands-on Labs & Workshops**: Practical exercises using **blockchain explorers**, **forensic tools**, and **smart contract analysis environments**.
- **Real-World Case Studies**: In-depth analysis of major **blockchain security incidents** and **DApp exploits** to illustrate concepts.
- **Simulated Investigations**: Participants will engage in simulated **forensic investigations** of mock blockchain incidents.
- **Code Review Sessions**: Collaborative analysis of **vulnerable smart contract code**.
- **Q&A and Discussion Forums**: Encouraging interaction and knowledge sharing among participants and instructors.
- **Capstone Project**: A practical, comprehensive investigation of a simulated or real-world **smart contract security incident**.

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