Training Course on Investigating Cryptocurrency and Blockchain-Related Crimes

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid proliferation of **cryptocurrencies** and **blockchain technology** has revolutionized global finance, yet it also presents unprecedented challenges for law enforcement, financial institutions, and regulatory bodies. Training Course on Investigating Cryptocurrency and Blockchain-Related Crimes is meticulously designed to equip participants with the critical knowledge and practical skills required to effectively **investigate**, **trace**, and **prosecute illicit activities** leveraging these digital assets. From sophisticated **cybercrimes** and **money laundering** to **fraud schemes** and **dark web transactions**, understanding the intricate workings of decentralized ledgers is paramount in today's evolving digital threat landscape.

This comprehensive program delves into the foundational principles of blockchain, **cryptographic security**, and various cryptocurrency ecosystems, highlighting their vulnerabilities to criminal exploitation. Through **hands-on exercises** and **real-world case studies**, attendees will master advanced **blockchain forensics techniques**, learn to utilize specialized **on-chain analysis tools**, and develop strategies for **digital evidence collection** and preservation. By fostering a deep understanding of the **pseudo-anonymous nature** of cryptocurrency transactions and the legal frameworks surrounding them, this course empowers investigators to dismantle criminal networks and safeguard the integrity of the digital economy.

Programme Curriculum

Training Course on Investigating Cryptocurrency and Blockchain-Related Crimes

Introduction

The rapid proliferation of **cryptocurrencies** and **blockchain technology** has revolutionized global finance, yet it also presents unprecedented challenges for law enforcement, financial institutions, and regulatory bodies. Training Course on Investigating Cryptocurrency and Blockchain-Related Crimes is meticulously designed to equip participants with the critical knowledge and practical

skills required to effectively **investigate**, **trace**, and **prosecute illicit activities** leveraging these digital assets. From sophisticated **cybercrimes** and **money laundering** to **fraud schemes** and **dark web transactions**, understanding the intricate workings of decentralized ledgers is paramount in today's evolving digital threat landscape.

This comprehensive program delves into the foundational principles of blockchain, **cryptographic security**, and various cryptocurrency ecosystems, highlighting their vulnerabilities to criminal exploitation. Through **hands-on exercises** and **real-world case studies**, attendees will master advanced **blockchain forensics techniques**, learn to utilize specialized **on-chain analysis tools**, and develop strategies for **digital evidence collection** and preservation. By fostering a deep understanding of the **pseudo-anonymous nature** of cryptocurrency transactions and the legal frameworks surrounding them, this course empowers investigators to dismantle criminal networks and safeguard the integrity of the digital economy.

Course Duration

10 days

Course Objectives

1. Comprehend the core architecture, consensus mechanisms, and distributed ledger technology (DLT) underpinning cryptocurrencies.
2. Differentiate between various cryptocurrencies and their unique forensic characteristics.
3. Develop proficiency in tracing cryptocurrency transactions using advanced blockchain explorers and analytics platforms.
4. Recognize patterns of money laundering, terrorist financing, and illicit transactions on the blockchain.
5. Understand the role of cryptocurrencies in darknet marketplaces and learn techniques for intelligence gathering in covert environments.
6. Acquire specialized knowledge to investigate and mitigate cryptocurrency-related ransomware attacks and digital extortion.
7. Explore the emerging landscape of Decentralized Finance (DeFi) and Non-Fungible Token (NFT) related crimes and investigative methodologies.
8. Learn best practices for securely acquiring, preserving, and validating digital evidence from cryptocurrency platforms and devices.
9. Understand international and national laws, regulations (AML/CFT), and compliance requirements pertaining to cryptocurrency investigations.
10. Leverage Open-Source Intelligence (OSINT) tools and techniques to identify real-world entities linked to cryptocurrency addresses.
11. Analyze various cryptocurrency wallet types and obtain crucial data from centralized and decentralized exchanges.
12. Identify common cryptocurrency scams (e.g., Ponzi schemes, phishing, rug pulls) and develop strategies for victim restitution.
13. Prepare robust investigative reports and present compelling digital evidence for successful prosecution in crypto crime cases.

Organizational Benefits

- Equip teams with the specialized skills to proactively detect, analyze, and disrupt sophisticated cryptocurrency-related criminal enterprises.
- Strengthen an organization's ability to identify and mitigate risks associated with money laundering, fraud, and illicit financing involving digital assets.

- Ensure adherence to evolving Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations in the cryptocurrency space, minimizing legal and reputational risks.
- Streamline investigation processes through efficient use of blockchain intelligence tools and methodologies, saving time and resources.
- Develop a deeper understanding of attack vectors in the blockchain ecosystem, enabling better protection against cyber threats and asset loss.
- Demonstrate a proactive commitment to combating digital financial crime, fostering confidence among stakeholders and the public.
- Position the organization as a leader in addressing the complexities of the digital asset landscape, attracting top talent and fostering innovation.

Target Audience

1. Law Enforcement Officers.
2. Financial Intelligence Unit (FIU) Analysts
3. Anti-Money Laundering (AML) & Compliance Professionals.
4. Digital Forensic Investigators.
5. Prosecutors and Legal Professionals
6. Cybersecurity Specialists.
7. Fraud Investigators.
8. Regulatory Authorities.

Course Outline

Module 1: Introduction to Cryptocurrency and Blockchain Ecosystems

- Foundational Concepts.
- Key Cryptocurrencies
- Cryptographic Principles
- Blockchain Architecture
- Transaction Flow
- **Case Study:** The rise of Bitcoin and its early use cases, illustrating its initial adoption and potential for illicit activities.

Module 2: Cryptocurrency Wallets and Exchanges

- Wallet Types
- Exchange Types
- Wallet Forensics
- Exchange Data Collection
- Vulnerabilities
- **Case Study:** The Mt. Gox hack, analyzing the impact of exchange vulnerabilities on user funds and the subsequent investigations.

Module 3: On-Chain Analysis and Blockchain Explorers

- Introduction to On-Chain Data.
- Blockchain Explorers
- Address Clustering
- Transaction Graph Analysis
- Heuristics and Red Flags
- **Case Study:** Tracing funds from a publicized ransomware attack, demonstrating the step-by-step process of following the crypto trail.

Module 4: Advanced Blockchain Analytics Tools

- Specialized Software.
- Entity Recognition
- Transaction Flow Visualization
- De-anonymization Techniques
- Reporting and Exporting Data
- **Case Study:** Investigating a large-scale crypto Ponzi scheme using a commercial blockchain analytics tool to map out the financial network.

Module 5: Cryptocurrency in Money Laundering

- ML Typologies
- Mixing Services (Tumblers) & Privacy Coins
- Chain Hopping.
- Regulatory Landscape
- Financial Red Flags.
- **Case Study:** The AlphaBay darknet market takedown, showcasing how law enforcement tracked Bitcoin transactions to dismantle a major criminal enterprise.

Module 6: Dark Web and Illicit Marketplaces

- Dark Web Overview.
- Cryptocurrency as a Medium of Exchange.
- Intelligence Gathering
- Vendor and Buyer OpSec
- Law Enforcement Challenges
- **Case Study:** The Silk Road investigation, demonstrating how the FBI dismantled a major darknet marketplace and seized significant Bitcoin assets.

Module 7: Ransomware and Cyber Extortion

- Ransomware Ecosystem
- Negotiation & Payment
- Attribution & Decryption
- Incident Response.
- Preventative Measures
- **Case Study:** The Colonial Pipeline ransomware attack, analyzing the FBI's recovery of a significant portion of the Bitcoin ransom payment.

Module 8: Fraud Schemes and Scams in the Crypto Space

- Investment Scams
- Phishing & Social Engineering
- Romance Scams & Pig Butchering
- NFT and DeFi Scams.
- Victim Identification & Recovery
- **Case Study:** Analysis of a major "rug pull" event in the DeFi space, detailing how investigators identify the perpetrators and the challenges of asset recovery.

Module 9: Digital Evidence Collection and Preservation

- Legal Frameworks for Digital Evidence
- Identifying Digital Artifacts

- Forensic Imaging & Acquisition
- Data Preservation
- Courtroom Testimony.
- **Case Study:** Demonstrating the forensic acquisition of a compromised computer to extract cryptocurrency wallet files and transaction logs.

Module 10: Legal Frameworks and Regulatory Compliance (AML/CTF)

- International Standards
- National Regulations
- KYC/AML Best Practices.
- Jurisdictional Challenges
- Sanctions Evasion.
- **Case Study:** Examining a recent regulatory enforcement action against a non-compliant crypto exchange, highlighting the importance of robust AML programs.

Module 11: OSINT for Crypto Investigations

- Open-Source Data Sources
- Correlating On-Chain and Off-Chain Data
- Advanced Search Techniques
- Geolocation & Timelines
- Ethical Considerations & Privacy
- **Case Study:** Using OSINT to identify the individual behind a series of cryptocurrency phishing attacks, demonstrating the power of public data.

Module 12: Emerging Trends and Future Challenges

- Central Bank Digital Currencies (CBDCs)
- Quantum Computing
- Decentralized Autonomous Organizations (DAOs)
- Cross-Chain Interoperability
- AI and Machine Learning in Forensics
- **Case Study:** Discussing a hypothetical future scenario involving quantum-resistant cryptocurrency and the investigative challenges it poses.

Module 13: Courtroom Preparation and Expert Testimony

- Report Writing.
- Exhibit Preparation.
- Expert Witness Testimony.
- Challenging Digital Evidence
- Case Law and Precedent
- **Case Study:** Role-playing a courtroom scenario where participants present their investigative findings and are cross-examined on their methodology and conclusions.

Module 14: Practical Application and Simulation

- Simulated Crypto Crime Scenario
- Hands-on Tool Usage
- Evidence Handling Practice
- Collaborative Problem Solving
- Debrief and Feedback

- **Case Study:** A full-day practical simulation of a real-world cryptocurrency theft, where teams apply all learned techniques to solve the case.

Module 15: Professional Development and Resources

- Continuing Education
- Professional Certifications
- Networking Opportunities
- Resources for Investigators
- Ethical Guidelines
- **Case Study:** Discussing the ethical dilemmas faced by investigators in high-profile crypto cases, such as balancing privacy concerns with investigative needs.

Training Methodology

- **Instructor-Led Sessions:** Expert-led presentations and in-depth discussions on core concepts.
- **Hands-on Labs:** Practical exercises using real-world blockchain data and industry-standard investigation tools.
- **Case Study Analysis:** Detailed examination of actual cryptocurrency crime cases to illustrate theoretical concepts and practical applications.
- **Interactive Workshops:** Group activities and problem-solving scenarios to foster collaborative learning.
- **Simulated Investigations:** Realistic mock crime scenarios where participants apply their learned skills from evidence collection to reporting.
- **Upcoming Scheduled Sessions**

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Register Online Now

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