# Security and Privacy in Blockchain Applications 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

In an increasingly digitized and decentralized world, Blockchain Technology has emerged as a foundational layer for innovation across finance, supply chain, and identity management. This power, however, comes with complex risks. The need for Robust Security and Data Privacy has never been more critical, especially with the rise of decentralized finance (DeFi) and enterprise applications. Security and Privacy in Blockchain Applications Training Course provides a deep dive into securing decentralized systems, moving beyond theoretical concepts to focus on practical, real-world Threat Mitigation and Cryptographic Assurance. It addresses the inherent tension between a public ledger's transparency and the essential need for user and transaction confidentiality.

Security and Privacy are no longer optional features but non-negotiable requirements for successful blockchain adoption. The current landscape is plagued by sophisticated attacks on Smart Contracts, vulnerabilities in Layer-2 Solutions, and challenges in maintaining Regulatory Compliance (like GDPR) within decentralized frameworks. This training equips technical professionals with the advanced knowledge of Zero-Knowledge Proofs, secure Wallet Management, and DApp Auditing necessary to build, deploy, and manage trustworthy blockchain applications. Graduates will become indispensable assets in safeguarding digital assets and ensuring the long-term viability of Web3 initiatives.

## Programme Curriculum

**Security and Privacy in Blockchain Applications Training Course**

**Introduction**

In an increasingly digitized and decentralized world, Blockchain Technology has emerged as a foundational layer for innovation across finance, supply chain, and identity management. This power, however, comes with complex risks. The need for Robust Security and Data Privacy has never been more critical, especially with the

rise of decentralized finance (DeFi) and enterprise applications. Security and Privacy in Blockchain Applications Training Course provides a deep dive into securing decentralized systems, moving beyond theoretical concepts to focus on practical, real-world Threat Mitigation and Cryptographic Assurance. It addresses the inherent tension between a public ledger's transparency and the essential need for user and transaction confidentiality.

Security and Privacy are no longer optional features but non-negotiable requirements for successful blockchain adoption. The current landscape is plagued by sophisticated attacks on Smart Contracts, vulnerabilities in Layer-2 Solutions, and challenges in maintaining Regulatory Compliance (like GDPR) within decentralized frameworks. This training equips technical professionals with the advanced knowledge of Zero-Knowledge Proofs, secure Wallet Management, and DApp Auditing necessary to build, deploy, and manage trustworthy blockchain applications. Graduates will become indispensable assets in safeguarding digital assets and ensuring the long-term viability of Web3 initiatives.

**Course Duration**

5 days

**Course Objectives**

1. Analyze the cryptographic foundations of Immutable Ledgers and their security implications.
2. Evaluate and mitigate vulnerabilities in major Smart Contract platforms, focusing on reentrancy and overflow.
3. Implement best practices for Decentralized Identity (DID) and secure Key Management systems.
4. Master the application of Zero-Knowledge Proofs (ZKPs) and other Privacy-Enhancing Technologies (PETs) to ensure data confidentiality.
5. Develop robust Threat Models for decentralized applications (DApps) and DeFi Protocols.
6. Audit blockchain network security against common threats like 51% Attacks and Sybil attacks.
7. Design secure and Quantum-Resistant cryptographic protocols for future-proofing blockchain systems.
8. Formulate strategies for achieving GDPR-Aligned data handling on public and permissioned blockchains.
9. Utilize security tools for automated Smart Contract Auditing and Vulnerability Scanning.
10. Assess the security of Cross-Chain Bridges and Interoperability Solutions against emerging risks.
11. Implement secure Governance Models to prevent central point-of-failure attacks.
12. Differentiate security models between Public, Private, and Hybrid Blockchains
13. Create an effective Incident Response Plan for post-exploitation analysis and recovery of a compromised blockchain application.

**Target Audience**

1. Blockchain Developers and Engineers
2. Cybersecurity Professionals and Security Architects
3. IT Risk & Compliance Managers
4. Smart Contract Auditors and Penetration Testers
5. Technical Project Managers overseeing blockchain initiatives
6. DevOps Engineers deploying decentralized applications
7. Enterprise Architects designing internal ledger systems
8. RegTech Specialists focused on crypto and data privacy regulations

**Course Modules**

**1. Foundational Cryptography and Blockchain Architecture Security**

- Review of Hash Functions and Digital Signatures in transaction security.
- Security analysis of Consensus Mechanisms
- Understanding the Blockchain Trilemma.
- Network-Level Attacks: Mitigation of Sybil, Eclipse, and 51% attacks.
- Case Study: The Ethereum Classic 51% Attacks

**2. Smart Contract Vulnerabilities and Auditing**

- Common exploit patterns
- Secure coding best practices and Formal Verification methods.
- Tools and techniques for Automated Security Scanning and fuzzing.
- Access control patterns and secure use of Oracles.
- Case Study: The DAO Hack

**3. Decentralized Finance (DeFi) Protocol Security**

- Flash Loan Attacks, Price Oracle Manipulation.
- Security of Yield Farming and Decentralized Exchange contracts.
- Risks of Token Standards and their extensions.
- Securing Liquidity Pools and automated market makers
- Case Study: The Cream Finance Exploit

**4. Advanced Privacy-Enhancing Technologies (PETs)**

- Theory and application of Zero-Knowledge Proofs.
- Confidential transactions and the role of Homomorphic Encryption.
- Privacy features in networks like Monero, Zcash, and rollups.
- Implementing Mixers and other transaction obfuscation techniques.
- Case Study: Privacy Leakage and De-anonymization on Public Ledgers

**5. Key Management and Wallet Security**

- Best practices for Private Key Storage.
- Security review of Custodial and Non-Custodial Wallets.
- Implementing Hierarchical Deterministic (HD) Wallets and recovery phrases.
- Securing Decentralized Identity (DID) and Self-Sovereign Identity (SSI).
- Case Study: Wallet Breaches and Seed Phrase Compromises

**6. Layer-2 Solutions and Interoperability Security**

- Security models of Layer-2 Scaling Solutions
- Vulnerabilities in Cross-Chain Bridges and asset wrapping.
- Trust and security in Interoperability Protocols
- Protecting off-chain components and Sidechains.
- Case Study: Major Cross-Chain Bridge Exploits

**7. Enterprise Blockchain and Regulatory Compliance**

- Security differences in Permissioned Blockchains.
- Meeting GDPR and other data regulations with blockchain.
- KYC/AML implementation in decentralized systems.
- Designing robust Governance Mechanisms and upgrade processes.

- Case Study: Implementing GDPR-Compliant Data Storage in a Private Enterprise Chain

**8. Incident Response, Forensics, and Future Threats**

- Developing a Blockchain Incident Response Plan
- Cryptocurrency Forensics and on-chain analysis for tracing illicit funds.
- The threat of Quantum Computing to current cryptography.
- Emerging risks in Web3 Ecosystems.
- Case Study: Post-Mortem Analysis of a Major DeFi Protocol Hack and Fund Tracing

### 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 |
|---|---|---|---|
| **21 Sep 2026** | 25 Sep 2026 | Online | $1,000 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $1,500 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |

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

**Register Online Now**

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