Co-funded by
the European Union

V2B: Creating NFT Opportunities on Metaverse for Art VET Trainees

UNIT 2: Security Strategy while using Blockchain

Trainer guidelines

Project Number: 2022-1-DE02-KA210-VET-000080828

Index

ACTIVITY 1: WORKSHOP FOR UNDERSTANDING BLOCKCHAIN TECHNOLOGY BASICS AND IMPORTANCE 2
ACTIVITY 2: SECURE CHAIN 5
ACTIVITY 3: HARDWARE WALLET DEMONSTRATION AND COMPARISON 8
ACTIVITY 4: PHISHING ATTACK SIMULATION 10
ACTIVITY 5: NFT DATA INTEGRITY WORKSHOP 12
ACTIVITY 6: TIPS FOR AVOIDING SCAMS AND FRAUDS IN THE BLOCKCHAIN WORKSHOP 14
ANNEX 22

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by
the European Union

ACTIVITY 1: WORKSHOP FOR UNDERSTANDING BLOCKCHAIN TECHNOLOGY BASICS AND IMPORTANCE

Abstract

In this activity, trainees will put to practice the content learned on "2.1 Understanding Blockchain Technology Basics and Importance" This activity provides a comprehensive understanding of blockchain technology, covering its basics and emphasizing its significance in various industries. Participants will delve into the genesis of blockchain, its diverse forms, architecture, security features, and practical applications across sectors. The workshop employs interactive discussions, hands-on activities, and guest speakers to facilitate an engaging learning experience.

Keywords

Blockchain Technology, Cryptocurrency, Smart Contracts, Node, Consensus, Security, Trust, Blockchain Types, Applications.

Duration

60 minutes

Learning Objectives

- Define blockchain technology and its fundamental components.
- Explain the architecture and various forms of blockchain networks.
- Understand the significance of security and trust in blockchain systems.
- Evaluate the potential benefits and challenges associated with implementing blockchain.

Necessary Equipment and Materials

- Internet – connected devices (computer, tablet, smartphone)
- Access to virtual platforms for interactive experiences.
- Online Resources: links to video/ multimedia.
- Presentation Slides
- Feedback Forms for learners to share feedback on the module

Task

The workshop comprises tasks designed to offer participants a thorough and hands-on exploration of the Blockcain essential elements.

Interactive Discussions:

Engage participants in discussions about the transformative impact of blockchain on trust and transactions. Explore the diverse forms of blockchain through active thinking exercises.

Indicative Topic for Discussion 1: Blockchain Types and Their Trade-offs: Initiate a discussion about the four types of blockchains (public, private, hybrid, consortium) and their unique characteristics. Encourage participants to weigh the trade-offs associated with each type, considering factors like security, speed, and accessibility.

Indicative Topic for Discussion 2: Blockchain in Healthcare: Managing Electronic Health Records: Facilitate a discussion about the application of blockchain in healthcare, focusing on how it can securely manage electronic health records. Discuss the benefits of patient control over medical data and increased efficiency for healthcare providers.

Indicative Topic for Discussion 3: Challenges and Opportunities in the Blockchain Landscape: Encourage participants to discuss the challenges faced by blockchain technology, such as scalability limitations, data privacy concerns, and regulatory compliance. Explore potential solutions and opportunities for further development.

Indicative Topic for Discussion 4: Security and Privacy Challenges in Blockchain: Facilitate a discussion on the security features of blockchain, such as decentralization and cryptographic hashing. Explore the challenges blockchain faces in maintaining data privacy, especially in the context of regulations like GDPR.

Hands-On Activities:

Facilitate practical tasks to reinforce theoretical concepts. Participants will engage in activities that simulate blockchain transactions and understand the roles of nodes, miners, and smart contracts.

Indicative Topic for Activity: Blockchain and Cryptocurrency Simulation:

Objective: Experience cryptocurrency transactions.

Activity: Use a simplified cryptocurrency simulation platform (Crypto Parrot https://cryptoparrot.com is the cryptocurrency simulator where each one can engage with the market and practice their strategies before moving on to the real deal) Participants can take on roles as buyers, sellers, and miners, experiencing the transaction process and witnessing how the blockchain ledger records each transaction.

Indicative Topic for Activity 2: Blockchain Security Simulation:

Objective: Explore security features and vulnerabilities in blockchain.

Activity: Create a simulated environment (https://simewu.github.io/blockchain-simulator- Blockchain Simulator is a tool used to simulate the behavior of Bitcoin (and other proof-of-work blockchains) from within the browser. This tool can generate network topologies, mimic the behavior of real nodes, simulate how these layouts affect the distributed consensus of the system as a whole, and measure the outcomes.) where participants attempt to tamper with a blockchain ledger. Discuss the cryptographic methods like digital signatures and hash functions that prevent tampering. Participants can experiment with the difficulty of altering a block once it's added to the chain.

Solution

The Blockchain Technology module unfolds as a comprehensive learning experience for participants. They collectively define blockchain technology through interactive discussions and hands-on activities, enhancing their understanding of blockchain components practically. Guest speakers contribute insights into blockchain security. Complemented by interactive discussions, these sessions allow participants to engage in active thinking exercises and discussions, guiding them to evaluate blockchain applications across industries and think critically about real-world use cases and challenges.

ACTIVITY 2: SECURE CHAIN

Abstract

In this activity, trainees will put to practice the content learned on "2.2 Key Security Concerns in the Blockchain Space" To educate participants on the fundamental security concerns within the blockchain space and explore potential solutions through interactive discussions and collaborative problem-solving.

Keywords

Blockchain Security, Cryptography, Smart Contracts, Decentralization, Consensus Mechanisms

Duration

60 minutes

Learning Objectives

- Recognize key security challenges in the blockchain space.
- Understand the role of cryptography in blockchain security.
- Explore vulnerabilities associated with smart contracts.
- Analyze the impact of decentralization on security.
- Evaluate different consensus mechanisms and their security implications.

Necessary Equipment and Materials

- Internet-connected devices (computer, tablet, or smartphone)
- Presentation slides
- Whiteboard or online collaboration tool
- Blockchain case studies for discussion

Task

The task involves organizing a workshop focused on educating participants about fundamental security concerns within the blockchain space. The workshop aims to foster interactive discussions and collaborative problem-solving sessions to explore potential solutions. Participants will delve into topics such as 51% attacks, double-spending, smart contract vulnerabilities, and private key management. Through breakout sessions, hands-on activities, and expert insights, the workshop aims to empower participants to critically analyze and address security challenges in the dynamic landscape of blockchain technology.

The ultimate goal is to enhance participants' understanding of blockchain security and encourage the development of practical solutions for a more secure blockchain ecosystem.

- Introduction to Blockchain Security
  - An introductory explanation is given by the educator leading the event to provide an overview of blockchain technology and its security model.
  - A brief explanation of Distributed ledger, decentralized management and consensus mechanisms is given by the educator leading the activity.

- Security Concerns Deep Dive
  - Participants are divided into small groups.
  - Each group is assigned a specific security issue (e.g. double spending, 51% attacks, smart contract vulnerabilities).
  - Groups conduct research on the topics given to them and prepare a short presentation.

- Interactive Group Presentations
  - Each group presents their findings, highlighting real-world examples and potential implications.
  - Discussions regarding the broader implications of each security issue are encouraged.

- Open Discussion and Q&A
  - Participants engage in an open discussion about emerging security issues and potential future threats.
  - Participants are allowed to ask questions and share their opinions.

- Solution Brainstorming
  - Participants are mixed and divided into new groups.
  - Each group brainstorms potential solutions to the security concerns presented.
  - Encourage creativity and critical thinking.

- Collaborative Solutions Presentation
  - Groups present their proposed solutions.
  - Facilitate a discussion on the feasibility and potential impact of these solutions.

- Closing Remarks
  - Summarize key takeaways.

- Provide resources for further learning on blockchain security.

Solution

This workshop is designed to actively engage participants in understanding and addressing key security concerns in the blockchain space through research, collaboration, and critical thinking. By presenting a diverse set of solutions, participants can gain insights into the multifaceted nature of blockchain security and contribute to ongoing efforts to enhance the robustness of blockchain systems.

Co-funded by
the European Union

ACTIVITY 3: HARDWARE WALLET DEMONSTRATION AND COMPARISON

Abstract

In this activity, trainees will put to practice the content learned on "2.3 Strategies to Secure Your NFTs and Blockchain Transactions" In this activity, students will engage in a hands-on demonstration and comparison of various hardware wallets such as Ledger, Trezor, KeepKey, and others. The focus will be on understanding the features, advantages, and disadvantages of each wallet type.

Keywords

Hardware Wallet, Cryptocurrency, Security, Comparison, Demonstration

Duration

60 minutes

Learning Objectives

- Understand the importance and functionality of hardware wallets in securing digital assets.
- Compare different hardware wallets based on security features, user interface, and compatibility.
- Develop critical thinking skills in evaluating the suitability of different wallets for various needs.

Necessary Equipment and Materials

- Examples of hardware wallets (Ledger, Trezor, etc.), either physical units or detailed specifications and images.
- Computers or devices with internet access for research.
- Presentation tools (projector, screen, etc.) for showcasing wallet features.

Task

- The task begins with students being divided into small groups, with each group assigned a specific hardware wallet like Ledger, Trezor, or KeepKey. Each group's first objective is to conduct thorough research on their assigned wallet. They should explore various aspects including but not limited to the security features, ease of use, compatibility with different cryptocurrencies, and customer support services of the wallet.
- Students are expected to gather comprehensive information about how these wallets function, the level of security they provide against different types of cyber threats, and their overall user experience. They should pay special attention to the unique selling points of each wallet and how it stands out from its competitors.
- Once the research phase is completed, each group will prepare a presentation. This presentation should not only cover the technical specifications and features of the wallet but also include a practical demonstration or a detailed walkthrough, supported by images, videos, or live demonstrations if the physical wallet is available. The group should also prepare to address potential real-life scenarios where their wallet would be the most suitable choice, considering various factors like user expertise, transaction frequency, and types of cryptocurrencies handled.
- Lastly, each group will present their findings to the class, ensuring they provide a clear, concise, and comprehensive overview of their assigned hardware wallet. This presentation should be designed to educate their peers about the wallet and help them make an informed decision about which hardware wallet might be best suited for their needs.

Solution

After all groups have presented, the class will engage in a comparative discussion, guided by the trainer, to consolidate their understanding of the different hardware wallets. This discussion will help students form a comprehensive view of the available options for securely storing digital assets and how to choose the appropriate wallet for their needs.

ACTIVITY 4: PHISHING ATTACK SIMULATION

Abstract

In this activity, trainees will put to practice the content learned on "2.3 Strategies to Secure Your NFTs and Blockchain Transactions" This activity involves a simulation of a phishing attack where students must identify and respond to a mock phishing scenario. The aim is to enhance their awareness and ability to recognize and protect against real-life phishing attacks.

Keywords

Phishing, Cybersecurity, Simulation, Digital Literacy, Critical Thinking

Duration

60 Minutes

Learning Objectives

- Recognize the characteristics of phishing attacks.
- Develop critical thinking skills to identify and respond to cybersecurity threats.
- Enhance awareness of digital safety and personal information security.

Necessary Equipment and Materials

- Mock phishing emails or messages prepared by the trainer.
- Computers or devices for students to view and analyze the mock phishing content.
- Guidelines or checklists for identifying phishing attempts.

Task

- This task involves a practical exercise where students are exposed to mock phishing scenarios. The trainer will prepare and distribute a series of simulated phishing emails or messages, each designed to mimic the tactics real phishers use. These might include urgent language, requests for sensitive information, suspicious links, or misleading sender addresses.
- Students will individually review each message and use their critical thinking skills to identify signs of phishing. They must analyze the content, format, language, and any embedded links

or attachments in the emails or messages. Students should look for red flags such as spelling mistakes, generic greetings, and unusual requests for personal or financial information.

- The main part of the task is for students to write a brief analysis of each message, explaining why they believe it is a phishing attempt or a legitimate communication. They should reference specific elements of the message that contributed to their decision. Additionally, students will discuss the appropriate steps to take in response to each identified phishing attempt, which includes not clicking on any links, verifying the sender's authenticity, and reporting the phishing attempt to the appropriate authorities or service providers.
- After completing their analyses, students will share their findings with the class. This sharing session should involve a discussion about the different tactics phishers use and the best practices for identifying and avoiding phishing attacks. Students are encouraged to share any personal experiences or knowledge they have regarding phishing, fostering a collaborative learning environment.

Solution

Upon completing the analysis, students will share their findings and discuss the methods they used to identify the phishing attempts. The trainer will review the students' responses, providing feedback and further clarifying how to recognize and protect against phishing attacks. This debriefing session ensures that students understand the importance of cybersecurity and are equipped with the skills to safeguard their digital information

ACTIVITY 5: NFT DATA INTEGRITY WORKSHOP

Abstract

In this activity, trainees will put to practice the content learned on "2.3 Strategies to Secure Your NFTs and Blockchain Transactions" This workshop focuses on the concept of data integrity in Non-Fungible Tokens (NFTs). Students will explore the unique digital signatures of NFTs and their implications in terms of authenticity and ownership.

Keywords

NFT, Data Integrity, Blockchain, Digital Signature, Workshop

Duration

60 Minutes

Learning Objectives

- Understand the concept of data integrity in the context of NFTs.
- Learn about the unique digital signatures associated with NFTs.
- Explore the implications of these signatures in terms of ownership and authenticity.

Necessary Equipment and Materials

- Examples and case studies of NFTs with unique digital signatures.
- Computers or devices with internet access for research and exploration.
- Presentation materials or whiteboard for illustrating concepts.

Task

- In this workshop, students will dive deep into the world of Non-Fungible Tokens (NFTs) and their unique digital signatures. The task starts with students researching various NFTs that are popular or notable in the market. They should look into how these NFTs are created, with a focus on understanding what digital signatures are and how they are attached to NFTs.
- Each student or group will select specific NFTs and study their digital signatures. They should explore how these signatures serve as proof of authenticity and ownership, what makes them

unique, and how they are verified on the blockchain. Students should also look into cases where the integrity of NFTs was crucial in establishing their value or resolving disputes.

- After the research phase, students will prepare a presentation or a report summarizing their findings. This presentation should explain the concept of digital signatures in NFTs, provide examples of NFTs with unique signatures, and discuss the role of these signatures in the broader context of digital assets. Students should aim to highlight the importance of data integrity in maintaining the trustworthiness and value of NFTs in the digital marketplace.
- Finally, each student or group will present their findings to the class. The presentations should be informative and engaging, offering insights into the technical and practical aspects of NFT data integrity. They should also encourage discussion among peers about the implications of digital signatures in the world of blockchain and digital assets.

Solution

After the presentations, the trainer will lead a discussion to deepen the understanding of the subject. This will include addressing any misconceptions, emphasizing key points about data integrity in NFTs, and exploring the potential future implications of this technology. The activity concludes with students gaining a comprehensive understanding of the role of digital signatures in NFTs and their significance in the digital asset world.

ACTIVITY 6: TIPS FOR AVOIDING SCAMS AND FRAUDS IN THE BLOCKCHAIN WORKSHOP

Abstract

In this activity, trainees will put to practice the content learned on "2.6 Tips for Avoiding Scams and Frauds in the Blockchain World". During the "Tips for Avoiding Scams and Frauds in the Blockchain World" workshop, learners will actively engage in a multifaceted learning experience designed to equip them with practical skills and knowledge in identifying, understanding, and mitigating potential threats in the blockchain domain. The workshop is structured around four main chapters, each focusing on distinct aspects of blockchain security.

Keywords

Blockchain, Scams, Frauds, Security, Legal Considerations, Compliance, Cryptocurrency Regulations, Government Agencies, International Variations.

Duration

60 minutes

Learning Objectives

- Identify Common Scams and Frauds in the Blockchain World.
- Understand the Tactics Used by Scammers and Fraudsters.
- Evaluate Blockchain Systems for Legality.
- Implement Strategies to Verify the Authenticity of Blockchain Systems.
- Develop an Understanding of Blockchain Security Best Practices.

Necessary Equipment and Materials

- Internet – connected devices (computer, tablet, smartphone)
- Access to virtual platforms for interactive experiences.
- Online Resources: links to video/ multimedia.
- Presentation Slides
- Feedback Forms for learners to share feedback on the module

Task

The workshop on "Tips for Avoiding Scams and Frauds in the Blockchain World" engages participants in various tasks to foster a comprehensive understanding of blockchain security. Participants are actively involved in interactive discussions, hands-on activities, and feedback sessions. Through these instructional strategies, participants delve into recognizing common scams, evaluating blockchain systems, implementing security measures, and understanding legal considerations. Trainers facilitate guest speaker sessions to provide expert insights. Practical examples, such as real-world case studies and exploration of successful and fraudulent blockchain projects, enhance participants' ability to apply evaluation criteria and identify red flags. The workshop encourages critical thinking, proactive security measures, and compliance awareness. Ultimately, participants emerge equipped with practical skills and knowledge to navigate the blockchain landscape securely, contributing to the integrity and trustworthiness of blockchain technologies.

Interactive Discussions:

Interactive discussions are a crucial part of a workshop, fostering engagement and enhancing participants' understanding. Here are some topics for interactive discussions that the trainer can initiate during the workshop:

Indicative Topic for Discussion1: Real-world Scenarios: Present hypothetical scenarios or case studies related to potential scams in the blockchain world. Encourage participants to analyze scenarios and discuss how they would approach them to avoid falling victim to fraud.
Below are three hypothetical scenarios related to potential scams in the blockchain world. Participants can analyze these scenarios and discuss how they would approach them to avoid falling victim to fraud. The goal is to encourage critical thinking and explore different perspectives on handling challenging situations:

Scenario 1: The Deceptive ICO

Imagine a blockchain project launching an Initial Coin Offering (ICO) promising extraordinary returns on investment. The project claims to have a revolutionary technology but provides little technical information in its whitepaper. The team members are anonymous, and there's no clear roadmap. The ICO attracts attention through aggressive marketing tactics, promising quick and guaranteed profits.

Discussion Points:

- How would you approach evaluating the legitimacy of this ICO?
- What red flags do you see in this scenario?

- What steps can investors take to verify the credibility of the project before investing?

Scenario 2: Fake Wallet Application

Participants come across a new cryptocurrency wallet application advertised on social media platforms. The wallet claims to offer unparalleled security features and convenient functionalities. However, upon closer inspection, users notice that the wallet asks for excessive permissions, including access to private keys. The app is not listed on reputable app stores, and its website lacks essential security information.

Discussion Points:

- How would you assess the legitimacy of this wallet application?
- What are the potential risks associated with granting excessive permissions to a cryptocurrency wallet?
- What measures can users take to ensure the security of their funds when using a new wallet?

Scenario 3: Pump and Dump Scheme on a Decentralized Exchange

A relatively unknown cryptocurrency is listed on a decentralized exchange. Suddenly, there is a surge in social media activity, with influencers promoting the coin and claiming it's the next big thing. The coin's value skyrockets within a short period. However, shortly after, the value plummets, leaving investors with significant losses. It appears to be a coordinated effort to manipulate the market.

Discussion Points:

- How can investors differentiate between genuine market enthusiasm and coordinated market manipulation?
- What steps can be taken to verify the credibility of social media influencers promoting specific cryptocurrencies?
- In a decentralized exchange environment, what regulatory measures could be put in place to prevent pump and dump schemes?

Indicative Topic for Discussion 2: Practical Security Measures:

Engage participants in a discussion about their current security practices when dealing with blockchain technology.

Brainstorm and compile a list of practical security tips that participants can implement to protect themselves from scams.

Please see below the list for the Trainer

N.	List of Practical Security Tips		YES √	NO√
1.	**Implement Two-Factor Authentication (2FA)**	**Use 2FA to add an extra layer of security to online accounts, reducing the risk of unauthorized access.**		
2.	**Regularly Update Software**	**Keep blockchain software, wallets, and related applications up to date to patch vulnerabilities and enhance security.**		
3.	**Verify Website Security**	**Before using any blockchain-related website or wallet, ensure it has a secure connection (HTTPS) and employs encryption protocols.**		
4.	**Use Hardware Wallets**	**Consider using hardware wallets for storing cryptocurrencies, providing an extra layer of protection against online threats.**		
5.	**Educate Yourself**	**Stay informed about the latest scams and fraud tactics in the blockchain space to recognize and avoid potential threats.**		
6.	**Vet Third-Party Applications**	**Before downloading any blockchain-related applications, verify their legitimacy, and only use trusted sources.**		

Hands-On Activities:

Practical exercises on implementing security measures like two-factor authentication.

Hands-on evaluation of blockchain systems using provided criteria.

Explore real-world case studies through practical examples.

Activity 1. Two-Factor Authentication (2FA) Implementation:

Objective:

Participants will actively set up and experience the implementation of Two-Factor Authentication (2FA) to enhance their understanding of this security measure.

Steps:

Introduction to 2FA:

Briefly explain the importance of 2FA in blockchain security.

Provide information on different 2FA methods: authenticator apps, hardware tokens, or biometric factors.

Guided Setup:

Instruct participants to enable 2FA on their blockchain-related accounts (e.g., cryptocurrency exchange, wallet).

Provide step-by-step guides or demonstrations for popular 2FA methods.

Verification Process:

Have participants complete a verification process using the 2FA method they've chosen.

Discuss their experiences and any challenges encountered.

Discussion:

Facilitate a discussion on the importance of 2FA, potential scenarios where it adds security, and how it aligns with the module's security tips.

Activity 2: Explore Real-World Case Studies:

Participants will delve into real-world case studies to understand the practical application of evaluation criteria and red flag identification.

Steps:

Present real-world case studies (e.g., Ethereum's success, Bitconnect's failure) outlined in the module.

Emphasize the importance of critical analysis and the application of evaluation criteria.

Indicative Case Studies for presentation

Case Study 1: Ethereum's Success Story		
Description	Ethereum is one of the most successful blockchain projects. It gained prominence for introducing smart contracts and decentralized applications (DApps). Participants will investigate how Ethereum's experienced team, detailed whitepaper, and well-planned roadmap contributed to its legitimacy and prominence in the blockchain space.	
Tasks for Participants		
1. Team Analysis	Explore the professional backgrounds and expertise of Ethereum's core team members.	Assess how the team's experience played a role in Ethereum's success.
2. Whitepaper and Roadmap Examination	Access Ethereum's whitepapers and roadmaps from the official website.	Evaluate the quality and clarity of the whitepapers and roadmaps.
3. Community Engagement	Investigate Ethereum's history and achievements.	Analyze community engagement and contributions to the project

Case Study 2: The Rise and Fall of Bitconnect		
Description	Bitconnect was a fraudulent cryptocurrency project that operated as a Ponzi scheme. Participants will analyze how Bitconnect lured investors with unrealistic profit claims and understand how it ultimately collapsed as a scam	
Tasks for Participants		
1. Scheme Structure Understanding	Explore the structure of Bitconnect's Ponzi scheme.	Identify key elements that contributed to the scheme's success initially
2. Collapse Analysis	Investigate the events leading to the collapse of Bitconnect.	Analyze the aftermath and legal actions taken against the project

Case Study 3: The Case of OneCoin		
Description	OneCoin is another notorious example of a fraudulent blockchain project. Participants will investigate how OneCoin's founder, Ruja Ignatova, created a fictitious blockchain and issued a fraudulent cryptocurrency, leading to her disappearance and ongoing investigations	
Tasks for Participants		
1. Fictitious Blockchain Examination	Investigate how Ruja Ignatova created a fictitious blockchain for OneCoin.	Discuss the technical aspects of the deception
2. Issuance of Fraudulent Cryptocurrency	Analyze how OneCoin issued a fraudulent cryptocurrency	Discuss the impact on investors and the wider blockchain community
3. Founder's Disappearance and Investigations	Explore the circumstances surrounding Ruja Ignatova's disappearance	Investigate ongoing legal actions and investigations related to OneCoin

Group Exploration:

Divide participants into groups and assign each group a case study to explore in-depth.

Instruct them to gather additional information beyond what is provided in the module.

Group Presentations:

Each group presents their findings, discussing how the project aligns with the evaluation criteria and identifying key factors contributing to success or failure.

Discussion and Comparison:

Facilitate a discussion comparing different case studies.

Discuss commonalities and differences in evaluating successful and fraudulent blockchain projects.

Feedback Sessions:

Conduct feedback sessions after practical examples to assess learners' understanding **(Annex I)**

Encourage learners to share their experiences and insights.

Solution

The learners will actively participate in discussions, hands-on activities, and practical evaluations. They will analyze case studies, engage with experts, and receive feedback on their understanding. The multifaceted approach ensures that learners not only gain theoretical knowledge but also develop practical skills to navigate the complex landscape of blockchain security, fraud prevention, and legal considerations.

ANNEX

Annex I: Evaluation Form for Activity 6

1. Understanding of Scams and Frauds:

How well did the module cover common scams and frauds in the blockchain world?

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

2. Two-Factor Authentication (2FA) Activity:

Rate your experience with the hands-on 2FA implementation activity.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

3. Hands-On Evaluation of Blockchain Systems:

Evaluate the effectiveness of the hands-on blockchain system evaluation.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

4. Exploration of Real-World Case Studies:

Rate the usefulness of the real-world case studies in understanding blockchain security.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

5. Encouragement to Share Experiences and Insights:

Rate how well the module encouraged participants to share their experiences.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

6. Legal Challenges and International Variations Discussion:

Evaluate the depth and relevance of the legal discussions in the module.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

7. Overall Satisfaction with the Module:

Rate your overall satisfaction with the blockchain security module.

Excellent	Good	Satisfactory	Needs Improvement	Poor

Comments:

8. Additional Comments and Suggestions for Improvement:

Thank you for sharing your feedback! Your insights are crucial for enhancing our training programs.