AVENQOR
EDUCATION ONLY

Crypto Basics: Exchanges, Wallets, On-Chain vs Off-Chain

Security-first crypto foundation: exchanges vs wallets, custody, and on-chain/off-chain in plain language.

Build a solid foundation in cryptocurrency with a focus on security.

Crypto Basics | Exchanges | Wallets | On-Chain | Off-Chain

AVENQOR

Legal and Risk Notice

- This course is for educational purposes only and does not provide financial advice.
- Cryptocurrency trading is highly speculative and involves risk of loss.
- No guarantees of performance or success are made in this course.
- Always conduct your own research before making any trading decisions.
- This course does not endorse any specific exchanges, wallets, or trading platforms.

Who This Is Not For

- Individuals seeking specific investment advice.
- Traders looking for guaranteed returns.
- Those unwilling to accept the risks associated with cryptocurrency trading.

AVENQOR

How to Use This Course

Recommended Pace

- Complete one module per week for thorough understanding.
- Review lessons multiple times for better retention.
- Engage with exercises to reinforce learning.

Instructions

- Read each lesson carefully and take notes.
- Complete the exercises at the end of each module.
- Use the glossary for unfamiliar terms.
- Review the risk box to understand potential pitfalls.
- Utilize the one-page summary for quick reference.
- Take the self-test quiz to assess your understanding.

This course is designed to be print-friendly for offline study.

Keep a journal of your learning and reflections on cryptocurrency.

Schedule regular reviews of the material to reinforce knowledge.

AVENQOR

Table of Contents

Each entry links to a specific module or lesson.

AVENQOR

Preface / Orientation

Who This Is For

- Complete beginners interested in cryptocurrency.
- Self-taught users seeking structured knowledge.
- Individuals wanting to understand crypto security fundamentals.

What You Will Learn

- The differences between exchanges and wallets.
- How custody models work and their trade-offs.
- The basics of on-chain and off-chain transactions.
- The importance of keys and seed phrases.
- Best practices for account hygiene.
- Common mistakes to avoid in crypto trading.

What This Course Will Not Do

- Provide specific investment advice or recommendations.
- Guarantee any profits or performance.
- Offer real-time trading signals or calls.
- Substitute for professional financial advice.

Prerequisites

- No prior knowledge of cryptocurrency is required.
- A willingness to learn and engage with the material.

AVENQOR

Understanding Exchanges and Wallets

Goal: To differentiate between exchanges and wallets, highlighting their purposes and associated risks.

What are Exchanges?

Exchanges are platforms where you can buy, sell, or trade cryptocurrencies. They act as intermediaries between buyers and sellers.

Exchanges can be centralized (managed by a company) or decentralized (operating without a central authority).

> Centralized Exchange: A platform that matches buyers and sellers and holds users' funds.

> Decentralized Exchange: A platform that allows peer-to-peer trading without an intermediary.

Understanding the type of exchange you are using is crucial for assessing risk.

Why it matters: Knowing the difference helps you choose the right platform for your trading needs.

What are Wallets?

Wallets store your cryptocurrencies. They can be software-based (online) or hardware-based (offline).

> Software Wallet: A digital wallet that is accessible via the internet.

> Hardware Wallet: A physical device that securely stores your private keys offline.

Wallets do not trade cryptocurrencies; they simply hold them.

Why it matters: Understanding wallets is essential for securing your assets.

Risk Box: Using an insecure wallet can lead to loss of funds.

Exchanges vs Wallets

A visual comparison of exchanges and wallets, highlighting their purposes and risks.

Module 1 Checklist

- Identify the type of exchange you plan to use.
- Choose a secure wallet for your cryptocurrencies.
- Understand the risks associated with both exchanges and wallets.
- Review the differences between centralized and decentralized exchanges.
- Ensure you have a backup of your wallet's recovery phrase.
- Familiarize yourself with the fees associated with exchanges.

- Research the security measures of your chosen exchange.

Module 1 Exercise

Purpose: To reinforce understanding of exchanges and wallets.

1. List the exchanges you are considering and their features.
2. Identify the type of wallet you will use and its security features.
3. Create a pros and cons list for your chosen exchange and wallet.
4. Discuss your choices with a peer or in a study group.
5. Reflect on how you will manage risks associated with your choices.

Expected Output: A clear understanding of your chosen exchange and wallet, along with a risk management strategy.

Module 1 Risk Box

- Using an unregulated exchange can lead to loss of funds.
- Storing funds in a software wallet increases exposure to hacking.
- Not backing up your wallet can result in permanent loss of access.
- Failing to understand exchange fees can lead to unexpected costs.

Key Takeaways

- Exchanges facilitate trading but come with risks.
- Wallets are essential for securing your cryptocurrencies.
- Understanding the differences helps mitigate risks.
- Always prioritize security when choosing an exchange or wallet.
- Research thoroughly before making any decisions.

AVENQOR

Custody Models Explained

Goal: To explain the trade-offs between self-custody and third-party custody of cryptocurrencies.

Self-Custody

Self-custody means you control your private keys and funds.

This method provides full control but also places the responsibility for security on you.

Why it matters: Understanding self-custody is crucial for maintaining control over your assets.

Risk Box: Losing your private keys means losing access to your funds permanently.

Common mistake: Failing to back up your wallet can lead to irreversible loss.

Example: If you forget your wallet password or lose your device, you cannot recover your funds.

Third-Party Custody

Third-party custody involves entrusting your assets to a service provider.

This can provide convenience but also introduces risks, such as potential hacks or mismanagement.

Why it matters: Understanding third-party custody helps you assess the risks of relying on external services.

Risk Box: If the service provider is hacked, your funds may be at risk.

Common mistake: Not researching the security measures of the custody provider.

Example: If a custody provider suffers a data breach, your personal information and funds could be compromised.

Module 2 Checklist

- Evaluate your comfort level with self-custody.
- Research third-party custody options and their security measures.
- Understand the risks associated with both custody models.
- Decide which custody model aligns with your trading goals.
- Create a backup plan for your chosen custody method.
- Consider diversifying your assets across different custody models.
- Review the fees associated with third-party custody services.

Module 2 Exercise

Purpose: To evaluate your custody preferences.

1. List the pros and cons of self-custody versus third-party custody.
2. Identify which custody model you will use and why.
3. Discuss your choice with a peer or in a study group.
4. Reflect on how you will manage risks associated with your custody choice.
5. Create a backup plan for your custody method.

Expected Output: A clear understanding of your custody model choice and a risk management strategy.

Module 2 Risk Box

- Self-custody requires diligence and security awareness.
- Third-party custody can lead to loss of funds if the provider is compromised.
- Not having a backup plan can result in permanent loss of access.
- Failing to understand custody fees can lead to unexpected costs.

Key Takeaways

- Self-custody offers control but requires responsibility.
- Third-party custody provides convenience but comes with risks.
- Understanding custody models is essential for asset security.
- Always research custody options before making a decision.
- Create a backup plan for your chosen custody method.

AVENQOR

On-Chain vs Off-Chain Transactions

Goal: To clarify the differences between on-chain and off-chain transactions, including their implications for fees and confirmations.

On-Chain Transactions

On-chain transactions occur directly on the blockchain.

These transactions require network confirmations, which can take time and incur fees.

Why it matters: Understanding on-chain transactions is crucial for assessing transaction costs and time.

Risk Box: High network congestion can lead to increased fees and delays.

Example: During peak times, on-chain transaction fees can spike, making it expensive to send funds.

Common mistake: Not accounting for transaction fees when sending funds.

Off-Chain Transactions

Off-chain transactions occur outside the blockchain, often using a second layer or sidechain.

These transactions can be faster and cheaper but may sacrifice some security.

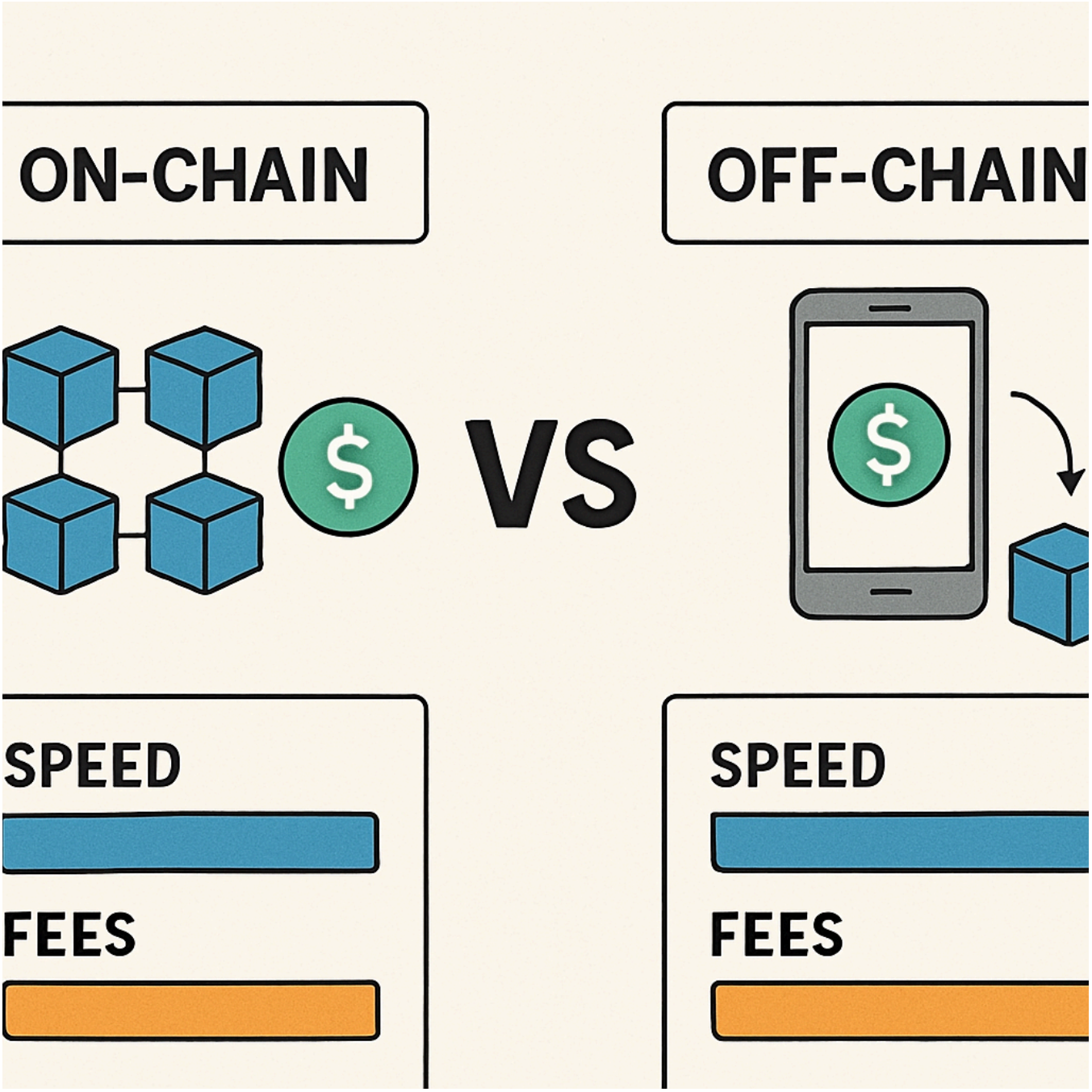
Why it matters: Understanding off-chain transactions helps you choose the right method for your needs.

Risk Box: Off-chain transactions can be less secure than on-chain transactions.

Example: If an off-chain solution is compromised, your funds could be at risk.

Common mistake: Assuming all off-chain transactions are secure.

On-Chain vs Off-Chain Transactions



A visual representation of the differences between on-chain and off-chain transactions, including speed and fees.

Module 3 Checklist

- Understand the differences between on-chain and off-chain transactions.
- Evaluate the fees associated with each transaction type.
- Consider the time required for confirmations in your decision-making.
- Choose the appropriate transaction type based on your needs.
- Research the security measures of off-chain solutions.
- Be aware of potential congestion on the blockchain.

- Review historical fee trends for on-chain transactions.

Module 3 Exercise

Purpose: To assess your understanding of transaction types.

1. List the advantages and disadvantages of on-chain and off-chain transactions.
2. Identify which transaction type you will use for different scenarios.
3. Discuss your choices with a peer or in a study group.
4. Reflect on how you will manage risks associated with your transaction choices.
5. Create a plan for monitoring transaction fees.

Expected Output: A clear understanding of when to use on-chain versus off-chain transactions.

Module 3 Risk Box

- On-chain transactions can incur high fees during congestion.
- Off-chain transactions may lack the same level of security as on-chain.
- Failing to understand transaction types can lead to unexpected costs.
- Not accounting for confirmation times can delay your trading strategy.

Key Takeaways

- On-chain transactions are secure but can be costly and slow.
- Off-chain transactions are faster but may sacrifice security.
- Choosing the right transaction type is essential for effective trading.
- Always consider fees and confirmation times in your decisions.
- Research transaction options before executing trades.

AVENQOR

Keys and Seed Phrases

Goal: To explain the importance of private keys and seed phrases in cryptocurrency security.

Understanding Private Keys

Private keys are cryptographic keys that allow you to access and control your cryptocurrencies.

Losing your private key means losing access to your funds permanently.

Why it matters: Understanding private keys is crucial for securing your assets.

Risk Box: Sharing your private key can lead to theft of your funds.

Example: If someone gains access to your private key, they can transfer your assets without your consent.

Common mistake: Storing private keys in insecure locations.

Understanding Seed Phrases

Seed phrases are a series of words that can be used to recover your wallet.

These phrases must be kept secure, as anyone with access can control your funds.

Why it matters: Understanding seed phrases is essential for wallet recovery.

Risk Box: Losing your seed phrase means losing access to your wallet.

Example: If you forget your seed phrase, you cannot recover your wallet.

Common mistake: Writing seed phrases down in insecure places.

Module 4 Checklist

- Secure your private keys and seed phrases.
- Understand the importance of keeping these secure.
- Create a backup plan for your seed phrase.
- Review the best practices for storing private keys.
- Educate yourself on the risks of sharing keys.
- Discuss key management strategies with peers.
- Regularly review your security practices.

Module 4 Exercise

Purpose: To reinforce understanding of keys and seed phrases.

1. Create a secure location for your private keys and seed phrases.
2. Write down your seed phrase and store it securely.
3. Discuss your key management strategies with a peer or in a study group.
4. Reflect on how you will manage risks associated with key loss.
5. Create a plan for regularly reviewing your key management practices.

Expected Output: A secure strategy for managing your private keys and seed phrases.

Module 4 Risk Box

- Losing your private key means losing access to your funds.
- Sharing your private key can lead to theft.
- Not securing your seed phrase can result in irreversible loss.
- Failing to regularly review your key management can lead to vulnerabilities.

Key Takeaways

- Private keys grant access to your funds and must be secured.
- Seed phrases are essential for wallet recovery.
- Understanding key management is critical for cryptocurrency security.
- Always prioritize the security of your keys and phrases.
- Regularly review your key management practices.

AVENQOR

Account Hygiene

Goal: To provide best practices for maintaining secure cryptocurrency accounts.

Password Management

Strong passwords are essential for protecting your accounts.

Use a combination of letters, numbers, and symbols.

Why it matters: A strong password is your first line of defense.

Risk Box: Weak passwords can be easily guessed or cracked.

Example: Using '123456' as a password makes your account vulnerable.

Common mistake: Reusing passwords across multiple accounts.

Two-Factor Authentication (2FA)

2FA adds an extra layer of security to your accounts.

This typically involves a code sent to your phone or email.

Why it matters: 2FA significantly reduces the risk of unauthorized access.

Risk Box: Not enabling 2FA can leave your account vulnerable.

Example: If someone knows your password but not your 2FA code, they cannot access your account.

Common mistake: Ignoring 2FA options when available.

Module 5 Checklist

- Create strong, unique passwords for each account.
- Enable 2FA on all accounts that offer it.
- Regularly update your passwords.
- Use a password manager to keep track of your passwords.
- Educate yourself on phishing attempts.
- Discuss account hygiene practices with peers.
- Review your account security regularly.

Module 5 Exercise

Purpose: To reinforce best practices for account hygiene.

1. Create strong passwords for your accounts.
2. Enable 2FA on your accounts.
3. Discuss your account hygiene practices with a peer or in a study group.
4. Reflect on how you will manage risks associated with account security.
5. Create a plan for regularly reviewing your account hygiene practices.

Expected Output: A secure strategy for maintaining account hygiene.

Module 5 Risk Box

- Weak passwords can lead to unauthorized access.
- Not enabling 2FA increases vulnerability.
- Ignoring account hygiene can result in loss of funds.
- Failing to regularly review your account security can lead to vulnerabilities.

Key Takeaways

- Strong passwords are essential for account security.
- 2FA adds an important layer of protection.
- Regularly reviewing account hygiene practices is crucial.
- Always prioritize security in your accounts.
- Educate yourself on potential threats to your accounts.

AVENQOR

Common Mistakes in Crypto Trading

Goal: To highlight common pitfalls and how to avoid them.

Phishing Scams

Phishing scams involve tricking you into revealing sensitive information.

These can come via email, social media, or fake websites.

Why it matters: Being aware of phishing scams can prevent loss of funds.

Risk Box: Falling for a phishing scam can lead to theft of your funds.

Example: Clicking on a link in a phishing email can compromise your account.

Common mistake: Not verifying the authenticity of communications.

Fake Support Scams

Fake support scams involve impersonating customer service representatives.

Scammers may ask for sensitive information or funds to 'help' you.

Why it matters: Recognizing fake support can protect your assets.

Risk Box: Providing information to fake support can lead to loss of funds.

Example: A scammer posing as support may ask for your private key.

Common mistake: Not verifying the identity of support personnel.

Module 6 Checklist

- Be aware of phishing tactics and how to recognize them.
- Verify the authenticity of any support communications.
- Educate yourself on common scams in the crypto space.
- Discuss potential scams with peers.
- Regularly review your security practices to avoid common mistakes.
- Stay informed about new scams and tactics.
- Use official channels for support inquiries.

Module 6 Exercise

Purpose: To reinforce awareness of common mistakes.

1. List common phishing tactics and how to avoid them.
2. Identify fake support scenarios you may encounter.
3. Discuss common mistakes with a peer or in a study group.
4. Reflect on how you will manage risks associated with scams.
5. Create a plan for staying informed about new scams.

Expected Output: A clear understanding of common mistakes and how to avoid them.

Module 6 Risk Box

- Falling for phishing scams can lead to loss of funds.
- Engaging with fake support can result in theft.
- Ignoring common mistakes increases vulnerability to scams.
- Failing to stay informed about scams can lead to significant losses.

Key Takeaways

- Phishing scams are a significant threat to crypto users.
- Recognizing fake support can protect your assets.
- Staying informed about common mistakes is crucial for security.
- Always verify the authenticity of communications.
- Educate yourself on potential scams and tactics.

AVENQOR

Security Checklist

Goal: To provide a comprehensive security checklist for cryptocurrency users.

Creating a Security Checklist

A security checklist helps ensure you take necessary precautions.

Include items like password strength, 2FA, and secure storage.

Why it matters: A checklist can help you stay organized and secure.

Risk Box: Neglecting security measures can lead to loss of funds.

Example: Forgetting to enable 2FA can leave your account vulnerable.

Common mistake: Failing to regularly update your checklist.

Reviewing Your Security Checklist

Regularly reviewing your security checklist ensures you stay secure.

Update it as needed based on new threats or changes in your situation.

Why it matters: Staying proactive can prevent security breaches.

Risk Box: Not reviewing your checklist can lead to vulnerabilities.

Example: If you change your password but forget to update your checklist, you may overlook security.

Common mistake: Ignoring the need for regular updates.

Module 7 Checklist

- Create a security checklist for your cryptocurrency accounts.
- Regularly review and update your checklist.
- Educate yourself on new security threats.
- Discuss your checklist with peers.
- Implement necessary changes based on your review.
- Stay informed about best practices for security.
- Use your checklist as a guide for daily security practices.

Module 7 Exercise

Purpose: To reinforce the importance of a security checklist.

1. Create your own security checklist for cryptocurrency accounts.
2. Review and discuss your checklist with a peer or in a study group.
3. Reflect on how you will manage risks associated with security.
4. Create a plan for regularly updating your checklist.
5. Implement changes based on your review.

Expected Output: A comprehensive and regularly updated security checklist.

Module 7 Risk Box

- Neglecting your security checklist can lead to vulnerabilities.
- Failing to update your checklist can expose you to risks.
- Not discussing security practices with peers can limit your knowledge.
- Ignoring new threats can lead to significant losses.

Key Takeaways

- A security checklist is essential for maintaining account security.
- Regular reviews help identify vulnerabilities.
- Staying informed about security threats is crucial.
- Always prioritize security in your cryptocurrency practices.
- Use your checklist as a daily guide.

AVENQOR

Before-Transfer Checklist

Goal: To provide a checklist to ensure safe cryptocurrency transfers.

Creating a Before-Transfer Checklist

A before-transfer checklist helps ensure safe transactions.

Include items like verifying addresses, double-checking amounts, and confirming network fees.

Why it matters: A checklist can prevent costly mistakes.

Risk Box: Failing to verify details can lead to irreversible loss.

Example: Sending funds to the wrong address can result in permanent loss.

Common mistake: Rushing through transfers without verification.

Reviewing Your Before-Transfer Checklist

Regularly reviewing your before-transfer checklist ensures you stay secure.

Update it as needed based on your experiences and lessons learned.

Why it matters: Staying proactive can prevent costly mistakes.

Risk Box: Not reviewing your checklist can lead to errors.

Example: If you forget to check the network fee, you may end up paying more than necessary.

Common mistake: Ignoring the need for regular updates.

Module 8 Checklist

- Create a before-transfer checklist for your cryptocurrency transactions.
- Regularly review and update your checklist.
- Educate yourself on common transfer mistakes.
- Discuss your checklist with peers.
- Implement necessary changes based on your review.
- Stay informed about best practices for safe transfers.
- Use your checklist as a guide for every transfer.

Module 8 Exercise

Purpose: To reinforce the importance of a before-transfer checklist.

1. Create your own before-transfer checklist for cryptocurrency transactions.
2. Review and discuss your checklist with a peer or in a study group.
3. Reflect on how you will manage risks associated with transfers.
4. Create a plan for regularly updating your checklist.
5. Implement changes based on your review.

Expected Output: A comprehensive and regularly updated before-transfer checklist.

Module 8 Risk Box

- Neglecting your before-transfer checklist can lead to costly mistakes.
- Failing to update your checklist can expose you to risks.
- Not discussing transfer practices with peers can limit your knowledge.
- Ignoring common transfer mistakes can lead to significant losses.

Key Takeaways

- A before-transfer checklist is essential for safe transactions.
- Regular reviews help identify potential errors.
- Staying informed about transfer practices is crucial.
- Always prioritize verification before making transfers.
- Use your checklist as a daily guide.

Glossary

Goal: To provide definitions of key terms used in the course.

Glossary of Terms

This glossary contains definitions of key terms used throughout the course.

Understanding these terms is essential for grasping the concepts discussed.

Example terms include: cryptocurrency, blockchain, wallet, exchange, private key, seed phrase.

Why it matters: Familiarity with terminology enhances comprehension.

Risk Box: Misunderstanding terms can lead to poor decision-making.

Common mistake: Not reviewing the glossary can limit understanding.

Using the Glossary

Refer to the glossary whenever you encounter unfamiliar terms.

This will help reinforce your understanding of the material.

Why it matters: Using the glossary can clarify concepts and improve learning.

Risk Box: Ignoring the glossary can hinder your learning process.

Example: If you don't understand 'blockchain', you may struggle with related concepts.

Common mistake: Not utilizing the glossary effectively.

Module 9 Checklist

- Review the glossary regularly to reinforce understanding.
- Use the glossary as a reference when studying.
- Discuss terms with peers to enhance comprehension.
- Create flashcards for key terms to aid memorization.
- Stay informed about new terms as the crypto landscape evolves.
- Regularly update your glossary knowledge.
- Engage with the material by applying terms in context.

Module 9 Exercise

Purpose: To reinforce understanding of key terms.

1. Create flashcards for key terms in the glossary.
2. Discuss terms with a peer or in a study group.
3. Reflect on how you will manage risks associated with misunderstanding terms.
4. Create a plan for regularly reviewing glossary terms.
5. Implement changes based on your review.

Expected Output: A solid understanding of key terms used in cryptocurrency.

Module 9 Risk Box

- Misunderstanding terms can lead to poor decision-making.
- Failing to review the glossary can limit comprehension.
- Not discussing terms with peers can hinder learning.
- Ignoring new terms can lead to gaps in knowledge.

Key Takeaways

- Understanding key terms is essential for grasping concepts.
- Regularly reviewing the glossary enhances comprehension.
- Using the glossary effectively can clarify complex ideas.
- Always prioritize understanding terminology in cryptocurrency.
- Engage with terms in context to reinforce learning.

AVENQOR

Self-Test Quiz

Goal: To assess your understanding of the course material.

Self-Test Quiz

This quiz consists of 15 questions covering key concepts from the course.

Use it to assess your understanding and identify areas for further study.

Why it matters: Self-testing reinforces learning and highlights knowledge gaps.

Risk Box: Not taking the quiz may result in unrecognized gaps in understanding.

Common mistake: Skipping the quiz can limit your learning.

Example questions include: What is a private key? What are the risks of using a centralized exchange?

Quiz Questions

1. What is the primary purpose of a cryptocurrency exchange?

a) To store cryptocurrencies

b) To facilitate the buying and selling of cryptocurrencies

c) To secure private keys

d) To create new cryptocurrencies

Correct answer: b) To facilitate the buying and selling of cryptocurrencies

Explanation: Exchanges are platforms that allow users to trade cryptocurrencies.

2. What is a common risk associated with using a centralized exchange?

a) High transaction fees

b) Lack of customer support

c) Potential for hacks and theft

d) Difficulty in trading

Correct answer: c) Potential for hacks and theft

Explanation: Centralized exchanges can be targets for hackers, leading to potential loss of funds.

3. What is a seed phrase?

a) A type of cryptocurrency

b) A series of words used to recover a wallet

c) A password for an exchange account

d) A transaction fee

Correct answer: b) A series of words used to recover a wallet

Explanation: Seed phrases are crucial for wallet recovery and must be kept secure.

4. What is the main advantage of using a hardware wallet?

a) It is free to use

b) It is connected to the internet

c) It stores private keys offline

d) It can create new cryptocurrencies

Correct answer: c) It stores private keys offline

Explanation: Hardware wallets provide enhanced security by keeping private keys offline.

5. Why is two-factor authentication important?

a) It makes transactions faster

b) It adds an extra layer of security

c) It eliminates the need for passwords

d) It is required by all exchanges

Correct answer: b) It adds an extra layer of security

Explanation: 2FA helps prevent unauthorized access to accounts.

6. What is the risk of using a software wallet?

a) It is too expensive

b) It can be hacked or compromised

c) It is difficult to use

d) It does not support all cryptocurrencies

Correct answer: b) It can be hacked or compromised

Explanation: Software wallets are vulnerable to online threats.

7. What should you do if you receive a suspicious email asking for your private key?

a) Reply to the email to ask for more information

b) Ignore the email and delete it

c) Provide the information to verify your account

d) Forward the email to customer support

Correct answer: b) Ignore the email and delete it

Explanation: This is likely a phishing attempt, and you should never share your private key.

8. What is a common mistake when transferring cryptocurrencies?

a) Verifying the recipient's address

b) Double-checking the transaction amount

c) Failing to check network fees

d) Using a secure wallet

Correct answer: c) Failing to check network fees

Explanation: Not accounting for fees can lead to unexpected costs.

9. What is the purpose of a security checklist?

a) To track your transactions

b) To ensure you take necessary security precautions

c) To manage your investments

d) To create new passwords

Correct answer: b) To ensure you take necessary security precautions

Explanation: A security checklist helps you stay organized and secure.

10. Why is it important to regularly review your security practices?

a) To increase transaction speed

b) To adapt to new threats and vulnerabilities

c) To reduce transaction fees

d) To improve customer service

Correct answer: b) To adapt to new threats and vulnerabilities

Explanation: Regular reviews help identify and mitigate risks.

11. What is a common risk of using a centralized exchange?

a) High transaction fees

b) Lack of customer support

c) Potential for hacks and theft

d) Difficulty in trading

Correct answer: c) Potential for hacks and theft

Explanation: Centralized exchanges can be targets for hackers.

12. What should you do if you forget your seed phrase?

a) Contact customer support for recovery

b) Try to guess it

c) Accept that you have lost access to your wallet

d) Write it down and store it securely

Correct answer: c) Accept that you have lost access to your wallet

Explanation: Seed phrases are essential for wallet recovery; losing it means losing access.

13. What is the main advantage of using a hardware wallet?

a) It is free to use

b) It is connected to the internet

c) It stores private keys offline

d) It can create new cryptocurrencies

Correct answer: c) It stores private keys offline

Explanation: Hardware wallets provide enhanced security.

14. What is a common mistake when using 2FA?

a) Enabling it on all accounts

b) Ignoring it when available

c) Using a weak 2FA method

d) Regularly updating your 2FA settings

Correct answer: b) Ignoring it when available

Explanation: Not enabling 2FA increases vulnerability.

15. Why is it important to educate yourself about common scams?

a) To improve trading skills

b) To avoid falling victim to scams

c) To increase transaction speed

d) To reduce fees

Correct answer: b) To avoid falling victim to scams

Explanation: Awareness of scams helps protect your assets.

Module 10 Checklist

- Take the self-test quiz to assess your understanding.
- Review any incorrect answers to identify knowledge gaps.

- Discuss quiz results with peers for further learning.
- Create a plan for further study based on your quiz performance.
- Regularly revisit quiz questions to reinforce learning.
- Stay informed about new developments in cryptocurrency.
- Engage with the material by applying concepts in practice.

Module 10 Exercise

Purpose: To assess your understanding of the course material.

1. Complete the self-test quiz.
2. Review your answers and explanations.
3. Discuss your results with a peer or in a study group.
4. Reflect on your learning and identify areas for improvement.
5. Create a plan for ongoing education in cryptocurrency.

Expected Output: A clear understanding of your strengths and weaknesses in the course material.

Module 10 Risk Box

- Not taking the quiz may result in unrecognized gaps in understanding.
- Failing to review quiz answers can limit your learning.
- Ignoring the need for ongoing education can lead to knowledge gaps.
- Not discussing results with peers can limit your perspective.

Key Takeaways

- Self-testing reinforces learning and highlights knowledge gaps.
- Regular review of quiz questions enhances retention.
- Engaging with peers can deepen understanding.
- Always prioritize continuous education in cryptocurrency.
- Use quizzes as a tool for self-assessment.

AVENQOR

One-Page Rules & Reality Check

Key Rules

- Always secure your private keys and seed phrases.
- Use strong, unique passwords for all accounts.
- Enable two-factor authentication wherever possible.
- Regularly review and update your security practices.

Reality Check

- Cryptocurrency trading is highly speculative and risky.
- Be aware of common scams and how to avoid them.
- Understand the differences between exchanges and wallets.
- Always verify transaction details before transferring funds.

Final Thoughts

- Education is key to successful trading.
- Stay informed about the evolving crypto landscape.
- Engage with the community for shared learning.
- Prioritize security in all your cryptocurrency activities.

Resources

- Utilize the glossary for unfamiliar terms.
- Refer to the checklist for security practices.
- Engage with peers for discussions and insights.
- Regularly revisit course material for reinforcement.

This summary provides key rules and realities to keep in mind while navigating cryptocurrency.

AVENQOR

Glossary

Cryptocurrency

A digital or virtual currency that uses cryptography for security.

Understanding cryptocurrency is fundamental to engaging with the crypto market.

Blockchain

A decentralized digital ledger that records transactions across many computers.

Blockchain technology underpins most cryptocurrencies and is crucial for understanding how they work.

Wallet

A digital tool used to store, send, and receive cryptocurrencies.

Knowing how wallets function is essential for securing your assets.

Exchange

A platform that facilitates the buying, selling, or trading of cryptocurrencies.

Understanding exchanges is vital for engaging in cryptocurrency trading.

Private Key

A secret number that allows you to access and control your cryptocurrency.

Securing your private key is crucial for protecting your funds.

Seed Phrase

A series of words used to recover a cryptocurrency wallet.

Keeping your seed phrase secure is essential for wallet recovery.

Two-Factor Authentication (2FA)

An extra layer of security requiring not only a password but also something that only the user has.

2FA significantly reduces the risk of unauthorized access to accounts.

Phishing

A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.

Recognizing phishing attempts is crucial for protecting your assets.

Custody

The responsibility for holding and safeguarding assets.

Understanding custody models helps you choose how to secure your cryptocurrencies.

On-Chain Transaction

A transaction that occurs directly on the blockchain.

On-chain transactions are secure but can incur higher fees.

Off-Chain Transaction

A transaction that occurs outside the blockchain, often using a second layer or sidechain.

Off-chain transactions can be faster and cheaper but may sacrifice some security.

Account Hygiene

Practices that ensure the security and integrity of your accounts.

Maintaining good account hygiene is essential for preventing unauthorized access.

Common Mistakes

Frequent errors made by users that can lead to loss or theft of funds.

Being aware of common mistakes helps you avoid them.

Security Checklist

A list of security measures to follow for protecting your cryptocurrency accounts.

A checklist helps ensure you take necessary precautions.

Before-Transfer Checklist

A list of steps to verify before executing a cryptocurrency transfer.

A before-transfer checklist can prevent costly mistakes.

Self-Custody

Controlling your own private keys and funds without relying on a third party.

Self-custody offers full control but requires responsibility for security.

Third-Party Custody

Entrusting your assets to a service provider for safekeeping.

Third-party custody can provide convenience but comes with risks.

AVENQOR

Self-Test Quiz

1. What is the primary purpose of a cryptocurrency exchange?

A. To store cryptocurrencies

B. To facilitate the buying and selling of cryptocurrencies ✓

C. To secure private keys

D. To create new cryptocurrencies

Explanation: Exchanges are platforms that allow users to trade cryptocurrencies.

2. What is a common risk associated with using a centralized exchange?

A. High transaction fees

B. Lack of customer support

C. Potential for hacks and theft ✓

D. Difficulty in trading

Explanation: Centralized exchanges can be targets for hackers, leading to potential loss of funds.

3. What is a seed phrase?

A. A type of cryptocurrency

B. A series of words used to recover a wallet ✓

C. A password for an exchange account

D. A transaction fee

Explanation: Seed phrases are crucial for wallet recovery and must be kept secure.

4. What is the main advantage of using a hardware wallet?

A. It is free to use

B. It is connected to the internet

C. It stores private keys offline ✓

D. It can create new cryptocurrencies

Explanation: Hardware wallets provide enhanced security by keeping private keys offline.

5. Why is two-factor authentication important?

A. It makes transactions faster

B. It adds an extra layer of security ✓

C. It eliminates the need for passwords

D. It is required by all exchanges

Explanation: 2FA helps prevent unauthorized access to accounts.

6. What is the risk of using a software wallet?

A. It is too expensive

B. It can be hacked or compromised ✓

C. It is difficult to use

D. It does not support all cryptocurrencies

Explanation: Software wallets are vulnerable to online threats.

7. What should you do if you receive a suspicious email asking for your private key?

A. Reply to the email to ask for more information

B. Ignore the email and delete it ✓

C. Provide the information to verify your account

D. Forward the email to customer support

Explanation: This is likely a phishing attempt, and you should never share your private key.

8. What is a common mistake when transferring cryptocurrencies?

A. Verifying the recipient's address

B. Double-checking the transaction amount

C. Failing to check network fees ✓

D. Using a secure wallet

Explanation: Not accounting for fees can lead to unexpected costs.

9. What is the purpose of a security checklist?

A. To track your transactions

B. To ensure you take necessary security precautions ✓

C. To manage your investments

D. To create new passwords

Explanation: A security checklist helps you stay organized and secure.

10. Why is it important to regularly review your security practices?

A. To increase transaction speed

B. To adapt to new threats and vulnerabilities ✓

C. To reduce transaction fees

D. To improve customer service

Explanation: Regular reviews help identify and mitigate risks.

11. What is a common risk of using a centralized exchange?

A. High transaction fees

B. Lack of customer support

C. Potential for hacks and theft ✓

D. Difficulty in trading

Explanation: Centralized exchanges can be targets for hackers.

12. What should you do if you forget your seed phrase?

A. Contact customer support for recovery

B. Try to guess it

C. Accept that you have lost access to your wallet ✓

D. Write it down and store it securely

Explanation: Seed phrases are essential for wallet recovery; losing it means losing access.

13. What is the main advantage of using a hardware wallet?

A. It is free to use

B. It is connected to the internet

C. It stores private keys offline ✓

D. It can create new cryptocurrencies

Explanation: Hardware wallets provide enhanced security.

14. What is a common mistake when using 2FA?

A. Enabling it on all accounts

B. Ignoring it when available ✓

C. Using a weak 2FA method

D. Regularly updating your 2FA settings

Explanation: Not enabling 2FA increases vulnerability.

15. Why is it important to educate yourself about common scams?

A. To improve trading skills

B. To avoid falling victim to scams ✓

C. To increase transaction speed

D. To reduce fees

Explanation: Awareness of scams helps protect your assets.