SECTION 4 REVIEW: WALLETS, TRANSACTIONS, AND SECURITY

A Prison Professors Self-Directed Course

Estimated time: 60–90 minutes

Educational Boundary:

> *This review provides general education about technology, risk, and preparation. It does not provide individualized financial, investment, legal, or tax advice.*

REVIEW PURPOSE

You have completed Lessons 12 through 15 of Understanding Web3. This review gives you a place to pause, strengthen your vocabulary, and connect the ideas of wallets, custody, transactions, security, privacy, and irreversible errors.

I encourage you to treat the review as part of the learning process rather than as a test of whether you remembered every sentence. Attempt each question first. When you find a gap, return to the lesson, examine the explanation, and revise your response. That process strengthens self-directed learning.

THE REVIEW COVERS:

- How wallets, public addresses, private keys, seed phrases, signatures, and authentication serve different functions.
- How custody and self-custody create different responsibilities, recovery challenges, and forms of counterparty risk.
- How a proposed blockchain transaction moves from preparation and authorization through broadcast, validation, confirmation, and finality.
- How phishing, impersonation, social engineering, privacy exposure, and irreversible errors can be reduced through disciplined verification.

HOW TO COMPLETE THE REVIEW

- Write your responses on separate paper or in an approved institutional messaging system.
- Number each response so that another person can follow your work.
- Complete the knowledge questions and vocabulary matching before reading the scenario.

» Explain your reasoning in your own words when a question asks why or asks you to evaluate a process.
» Use the printed lessons when you need to check a definition or reconsider an answer. You do not need the internet.
» Do not include passwords, private keys, seed phrases, authentication codes, account numbers, real wallet addresses, or other sensitive information.

The learner-facing review does not include answers. Correct responses, brief rationales, and sample responses will appear in the consolidated appendix after all lessons are completed. Attempt the work before consulting that appendix.

PART 1: KNOWLEDGE QUESTIONS

MULTIPLE CHOICE

1. Which statement best describes a blockchain wallet?
   a. A container that physically stores digital assets away from a blockchain
   b. A tool that helps a user view addresses, prepare transactions, and use signing credentials while the blockchain records the assets
   c. A public directory that proves the legal identity of every address holder
   d. A service that can reverse every transaction when a user makes an error
2. Which item is generally designed to be shared when receiving a digital asset?
   a. A public address
   b. A private key
   c. A seed phrase
   d. An authentication code
3. Which statement best describes a seed phrase?
   a. A public nickname for a wallet address
   b. A recovery secret that may recreate access to one or more accounts or keys
   c. A receipt proving that a transaction has reached finality
   d. A network fee paid to validators
4. Which statement offers the soundest comparison between custodial control and self-custody?
   a. Custodial control removes every risk because a service holds the credentials.
   b. Self-custody removes every risk because no outside service is involved.

c. Each arrangement places control, recovery duties, and risks in different hands, so a learner should evaluate the full arrangement instead of relying on a label.

d. The two arrangements are identical because all assets appear on a blockchain.

5. What does a valid digital signature normally show in a blockchain transaction?
   a. Someone with the relevant signing credential authorized the transaction data.
   b. The signer is the lawful owner of every asset connected with the address.
   c. The recipient is honest and the transaction is a wise decision.
   d. A network operator promises to reverse the transfer if a problem develops.
6. A transaction is successful on the network, but the sender used the wrong destination. Which description is most accurate?
   a. A successful network result proves the sender achieved the intended purpose.
   b. The network may have processed the instructions correctly even though the human outcome was unintended.
   c. The transaction fee guarantees that the destination will return the assets.
   d. Validation automatically corrects destination errors before confirmation.
7. You receive an urgent message from someone claiming to represent a familiar organization. The person asks you to use a supplied destination and share a secret to verify eligibility. What is the safest first response?
   a. Act quickly so the opportunity does not expire.
   b. Share part of the secret first and request proof later.
   c. Stop, verify the request through an independent channel, and seek help before authorizing anything.
   d. Forward the request to several friends so they can participate.

TRUE OR FALSE

» Control of a private key automatically proves the controller's legal identity and lawful ownership of every asset connected with the address.

» A public blockchain may expose transaction history and address relationships, while a finalized transfer may be difficult or impossible to reverse.

SHORT EXPLANATION

» A person says, “The address is visible on a block explorer, the wallet is described as cold storage, and the message uses a familiar logo. Those facts prove the request is authentic and safe.” In four to six sentences, explain what each fact may show, what it does not establish, and what the person should do before any transaction is authorized.

PART 2: VOCABULARY MATCHING

Match each term with the definition that best fits it. Write the letter of the term beside the correct numbered definition. Use each letter once.

TERMS

a. Wallet
b. Public address
c. Private key
d. Seed phrase
e. Self-custody
f. Counterparty risk
g. Transaction fee
h. Broadcast
i. Confirmation
j. Phishing
k. Social engineering
l. Irreversible transaction

DEFINITIONS

1. The act of sending a signed transaction to a blockchain network for processing.
2. The possibility that another person, company, or service will fail to perform as expected or will lose, misuse, freeze, or restrict assets.
3. A deceptive attempt to obtain sensitive information or induce an unsafe action through a fraudulent message, page, or communication.
4. A tool or interface that helps a user view blockchain information, prepare transactions, and use signing credentials.

5. A secret value used to create a digital signature and authorize actions connected with a blockchain address.
6. A network's recorded acceptance of a transaction into a block or its continued inclusion as additional blocks are added.
7. An arrangement in which a person or organization controls its own signing credentials instead of relying on a third-party custodian.
8. A sequence of recovery words that may recreate access to accounts or keys and must be protected as a powerful secret.
9. A transfer that, after sufficient network processing, generally cannot be canceled by a central help desk or automatically restored.
10. A shareable identifier used to receive assets or locate activity on a blockchain; it is not a password or proof of legal identity.
11. A charge paid for a network to process a transaction, commonly using the network's native asset.
12. The use of urgency, trust, fear, authority, curiosity, or other human reactions to persuade someone to reveal information or take an unsafe action.

PART 3: APPLIED SCENARIO — THE FALSE COMMUNITY MATCH REQUEST

This scenario is fictional. It does not describe a verified event involving Prison Professors, its supporters, or the independent PP token community.

A member of an education nonprofit receives a direct message from an account that copies the name, photograph, and logo of a person associated with the Prison Professors community. The message claims that an anonymous supporter will match a transfer to an education treasury if the team acts within 30 minutes.

The sender provides an unfamiliar destination and a button leading to a supplied page. The page asks the team member to connect a wallet, approve a contract request, and enter a seed phrase for "community verification." The sender says the request is safe because the treasury address is visible on a block explorer and the organization has previously described its resources as being held in cold storage.

The team member notices additional concerns:

» The request arrived through a channel the organization has never used for treasury instructions.
» No one has independently contacted the person whose name and image appear on the account.
» The destination has not been compared with a trusted record, and the selected network has not been confirmed.

» The contract request does not explain the amount or limits of the requested approval.
» The team has no written rule requiring a second reviewer before a treasury action.
» One person currently holds all signing authority, and the recovery process has not been documented for authorized team members.
» A public post connects the treasury address with the organization and discusses its approximate balance, creating privacy and targeting concerns.
» After the team member expresses doubt, another account offers to "recover" any assets lost during verification in exchange for an advance fee and authentication code.

No one has signed, broadcast, or authorized a transaction. The team pauses while there is still time to prevent an error.

SCENARIO QUESTIONS

1. Identify at least eight warning signs or safety failures in the scenario. For each one, explain the possible harm it could create.
2. Separate the information in the scenario into two categories: information that may be public and information that must remain secret. Explain why a public address or visible balance does not authenticate the sender.
3. Explain how the terms wallet, custody, self-custody, and cold storage apply to the scenario. What additional facts would you need before evaluating the team's control and recovery arrangement?
4. Place these transaction stages in a logical sequence: preparation, review, authorization by digital signature, broadcast, validation, confirmation, and finality. Identify the checkpoints at which the team can still stop and correct an error before broadcast.
5. Apply the Stop, Verify, Seek Help method. Describe the independent channels, trusted records, and authorized people the team should use before deciding whether the request is genuine.
6. Propose a short written safety process for future treasury requests. Include authorization, second review, destination and network checks, custody, recovery, privacy, suspicious-message escalation, and a rule against sharing secrets. Do not recommend a particular product or service.

COMPLETION CHECK

Before moving to Section 5, ask yourself whether you can:

- Distinguish a wallet, public address, private key, seed phrase, signature, and authentication control.
- Compare custody and self-custody without treating either arrangement as risk-free.
- Explain how control, recovery, counterparty exposure, and hot or cold storage answer different questions.
- Trace a transaction from preparation through finality and identify the points at which careful review can prevent an error.
- Recognize phishing, impersonation, social engineering, recovery scams, privacy exposure, and irreversible-error risks.
- Apply Stop, Verify, Seek Help before revealing information or authorizing an action.

If one statement remains difficult, return to the relevant lesson and write a brief explanation in your own words. That review shows that you are monitoring your understanding and strengthening your judgment.

SUBMISSION REMINDER

You may submit your completed review as a dated Profile journal entry, subject to your facility's rules. Include your name or approved Profile identifier, Understanding Web3 — Section 4 Review, and the date you completed the work.

Use one of the established Prison Professors Profile methods:

- Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Section 4 Review — [date completed].
- Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
- Send it to an approved family member or supporter who can enter it in your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, real wallet addresses, or other sensitive credentials in a Profile response.