LESSON 12: WALLETS, ADDRESSES, KEYS, AND SEED PHRASES

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational and Safety Boundary:

> *This lesson provides general education about blockchain access and digital security. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, exchange, device, network, company, or financial product. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson. Never place a real password, private key, seed phrase, authentication code, account number, or wallet address in a course response.*

OPENING GUIDANCE

In Lesson 9, we examined how a community used BNB Smart Chain to create a token connected with the Prison Professors mission. We also discussed a public treasury address that people could inspect through BscScan, a blockchain explorer. That public record can support transparency because anyone can examine activity associated with the address.

The public address does not give a visitor authority to move the assets. Control depends on private credentials that must remain secret. Those credentials do not appear on BscScan, and Prison Professors will never ask a participant to provide them.

That distinction gives us a practical reason to study wallets, addresses, private keys, and seed phrases. A person may share an address in an appropriate setting, just as an organization may publish a mailing address. A private key or seed phrase belongs in an entirely different category. Anyone who obtains that secret may be able to exercise control without the owner's permission.

I encourage you to learn the concepts without creating an account or handling any real credential. Understanding the responsibility comes before using the technology.

PURPOSE AND ESSENTIAL QUESTION

Lesson 12 corrects the misconception that a wallet physically stores digital assets. It explains how wallets help people view blockchain records, manage credentials, and authorize actions.

Essential Question:

» What information may be public, what information must remain private, and what responsibilities come with controlling digital credentials?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

» Explain what a blockchain wallet does and where digital-asset records exist.
» Distinguish a public address from a private key.
» Describe the purpose and sensitivity of a seed phrase.
» Explain how a digital signature can authorize an action without revealing the private key.
» Apply the rule that real keys, seed phrases, passwords, and authentication codes must never be requested, shared, or entered in course activities.

KEY TERMS

WALLET

Definition: A tool, application, or device that helps a person interact with blockchain accounts. Depending on its design, a wallet may display public records, prepare transactions, manage keys, and request signatures. The assets remain recorded on the blockchain rather than sitting inside the wallet.

Sample sentence: The wallet displayed the account balance by reading blockchain data and used the account's credentials to authorize a transaction.

PUBLIC ADDRESS

Definition: A public identifier used to locate an account or destination on a blockchain. An address may be shared when appropriate, but sharing it can expose transaction history and does not prove who controls it.

Sample sentence: The organization published a public address so observers could inspect activity without receiving authority to move the assets.

PRIVATE KEY

Definition: The secret part of a cryptographic key pair used to create digital signatures and authorize actions associated with an account. A private key must not be shared.

Sample sentence: The private key remained secret while the network verified the signature created with it.

SEED PHRASE

Definition: A sequence of words that some wallets use to generate or restore a set of keys. It is also called a recovery phrase or mnemonic phrase. Anyone who obtains it may be able to recreate the wallet's keys and control its accounts.

Sample sentence: The learner understood that a seed phrase was a powerful recovery secret, not an ordinary password or a course exercise.

SIGNATURE

Definition: A cryptographic result created with a private key to approve specific data, such as a transaction or message. A properly designed system can verify the signature without revealing the private key.

Sample sentence: The wallet asked the user to review the transaction details before creating a signature.

AUTHENTICATION

Definition: A process used to establish confidence that a person, device, or account has the authority or identity it claims. Proving control of a blockchain key does not automatically prove a person's legal identity.

Sample sentence: The application used a wallet signature for authentication, but the signature proved control of the key rather than the user's full identity.

MAIN LESSON

THE BLOCKCHAIN HOLDS THE RECORD; THE WALLET HELPS YOU INTERACT

A physical wallet may hold cash, identification, and cards. That familiar image creates a misleading idea when applied to blockchain technology. A blockchain wallet does not normally contain coins or tokens as objects inside a file or device.

The blockchain network maintains the account records. A wallet reads those records and provides tools for interacting with them. Depending on the wallet, a person may use it to:

- View balances and transaction history associated with an address.
- Generate or manage accounts and addresses.
- Prepare a transaction or other request.

» Review information that will be signed.
» Use a private key to create a digital signature.
» Send the signed request to a network or connected service.

The wallet is therefore closer to a control panel and key manager than a container of assets. If one compatible wallet application stops working, the blockchain record does not disappear. A person who still has the required credentials may be able to access the same account through another compatible tool.

The opposite is also important. Possessing a wallet application without the required credentials does not create control over an account. The interface and the authority are related, but they are not the same.

A PUBLIC ADDRESS IDENTIFIES A BLOCKCHAIN DESTINATION

A public address is used to identify an account or destination on a particular blockchain. Someone may provide an address to receive a transfer, and a blockchain explorer may display the history associated with that address.

An address is not the same thing as a private key. On networks such as Ethereum and BNB Smart Chain, account addresses are created from public-key information through cryptographic steps. The precise format differs among networks, so an address should always be considered together with the intended network.

Public does not mean harmless in every context. An address may reveal balances, transfers, timing, and connections with other addresses. If a person publicly connects an address with a name, business, location, or profile, observers may be able to study a larger pattern of activity. Blockchain addresses are often described as pseudonymous because the public record shows the address while the human identity may require outside evidence.

For that reason, a learner should understand two separate rules:

» A public address may be shared for a legitimate purpose after the network, recipient, and privacy consequences are considered.
» A real public address should not be included in a Prison Professors course response, because the assignment does not require it and the disclosure may connect learning records with financial activity.

A PRIVATE KEY PROVIDES SIGNING AUTHORITY

A private key is a large secret number used in public-key cryptography. Software normally handles it behind the scenes. The private key is mathematically connect-

ed with a public key, but the system is designed so that a person cannot practically calculate the private key from the public information.

The private key's central role is authorization. When a wallet signs a properly formed transaction, the signature allows the network to verify that the request came from someone with the corresponding private key and that the signed data was not changed after signing.

The private key should not be transmitted with the transaction. A properly designed signature process proves possession of signing authority without publishing the secret itself.

This design creates both power and risk. A network may accept a valid signature even when the human owner was deceived, pressured, careless, or unaware of what the interface displayed. Cryptography can verify that a key signed particular data. It cannot determine whether the person exercised good judgment.

A SIGNATURE IS AN ACTION, NOT A DECORATION

People sometimes see the word sign and think only of confirming a login. In Web3, a signature may authorize a transfer, approve a smart contract, accept terms, connect an account, or prove control of an address. The meaning depends on the exact data being signed.

I encourage learners to treat every signature request as an action that requires review. Ask:

- What application or person created the request?
- Which network and account are involved?
- What exact action will the signature authorize?
- Does the request include an amount, recipient, approval, deadline, or other condition?
- Can the information be verified through a trusted and independent source?
- Is there pressure to act quickly or ignore a warning?

A signature can be technically valid while the request is harmful. Later lessons will examine transactions and scams in more detail. The rule for this lesson is simple: never sign information that you do not understand.

A SEED PHRASE CAN RESTORE MANY KEYS

Managing a separate backup for every private key would be difficult. Many modern wallets use a deterministic process in which one starting secret can generate a connect-

ed set of keys. A seed phrase presents recovery information as an ordered list of words that a person can record more accurately than a long string of numbers and letters.

Under the widely used BIP-39 specification, a wallet-generated mnemonic may contain 12, 15, 18, 21, or 24 words. The phrase is converted into a seed, and another process may derive many keys from that seed. This technical distinction explains why the phrase can restore more than one account.

Not every wallet uses BIP-39 or any seed phrase. Wallet designs, recovery methods, and compatibility rules vary. A person should never assume that a phrase works with every wallet or that a password can replace it.

A seed phrase is extremely sensitive because it may provide access to every account derived from it. It should never be:

- Sent by email, text message, or social media.
- Entered into an unsolicited website or form.
- Read to a supposed support agent.
- Photographed or placed in a course assignment.
- Shared with Prison Professors, a teacher, a family member, or anyone claiming to verify a wallet.
- Created from a favorite quotation or a sentence invented by the user.

This lesson will not display an example seed phrase. A string of ordinary words can look harmless even though a real phrase may function as a master recovery secret.

PASSWORDS, AUTHENTICATION CODES, PRIVATE KEYS, AND SEED PHRASES HAVE DIFFERENT ROLES

THESE SECRETS ARE SOMETIMES CONFUSED:

- A password may unlock an application, account, encrypted file, or device. It does not necessarily recreate the blockchain keys.
- An authentication code is often a temporary code used as an additional proof during login or account recovery.
- A private key authorizes actions for a particular blockchain account or cryptographic identity.
- A seed phrase may restore a group of keys and accounts created from a common seed.

The recovery process depends on the custody arrangement and wallet design, which Lesson 13 will examine. A custodial service may offer password recovery because the service controls the underlying keys. A self-custody wallet may have no company capable of restoring access after the recovery information is lost.

Different roles do not change the safety rule. None of these secrets belongs in a course response, message to a stranger, or unverified website.

THE MAILBOX ANALOGY HELPS, BUT ONLY TO A POINT

Imagine a locked mailbox. The street address can be shared so people know where to deliver mail. The key should remain private because it opens the box.

This analogy helps distinguish a public address from a private credential. It also has limits. A blockchain address may reveal a lasting public history. A private key does not physically open a container; it creates mathematical signatures. A seed phrase may restore many keys rather than one lock. A blockchain network checks cryptographic rules rather than relying on a postal employee.

Use the analogy to begin understanding, then return to the precise concepts.

PUBLIC TRANSPARENCY DOES NOT REVEAL PRIVATE AUTHORITY

The Prison Professors community treasury provides a useful applied example. The community published a BNB Smart Chain address so observers could inspect activity through BscScan. A blockchain explorer can read the public ledger and display information connected with the address.

The explorer does not hold the assets, and the public address does not contain them. The blockchain records the account state. A wallet or signing system manages the credentials used to authorize actions.

The public record may show that an address received or sent assets. It does not prove by itself which human being controls the private credentials, whether a transfer followed an outside agreement, or how those credentials are protected. Those conclusions require additional evidence.

The case demonstrates a balanced use of public and private information:

- The public address can support observation and accountability.
- The private key or recovery information must remain confidential.
- Publishing the address does not publish signing authority.
- Protecting signing authority does not prevent public verification of the ledger.

We will continue using this case when discussing custody, transactions, smart contracts, and security. The purpose is education, not promotion of the PP token or any digital asset.

CONTROL OF A KEY IS NOT THE SAME AS PROOF OF IDENTITY OR ENTITLEMENT

A valid signature can show that someone controlled a particular private key when signing the data. It does not automatically prove that the signer is a named person, owns an outside asset, had legal authority, acted voluntarily, or deserved access to a service.

This boundary connects Lesson 12 with Lesson 11. A token may be controlled by an address, and an address may be controlled through a key. Outside evidence is still needed to connect the key with a person, organization, agreement, or legal right.

Responsible systems combine cryptography with policies, identity checks when appropriate, recovery procedures, access controls, and human accountability. Technology can verify a signature without answering every question about the signer.

APPLIED SCENARIO: PUBLIC ADDRESS, PRIVATE CONTROL

The scenario builds on the public Prison Professors community case discussed in Lesson 9. It does not reproduce the real treasury address, balance, or credentials.

A community publishes a BNB Smart Chain treasury address on its official information page. Supporters can enter that public address into BscScan and inspect the ledger history. A message then appears in a public chat:

Message received: "I work with the wallet provider. To confirm that the treasury belongs to your organization, send me the seed phrase and the latest authentication code. I will compare them with BscScan and place a verified label on the address."

The request contains several false or dangerous ideas.

- BscScan can display public address activity without receiving a seed phrase, private key, password, or authentication code.
- A seed phrase or private key is not evidence to send to a stranger. Sharing it may surrender control.
- An authentication code should not be sent to another person, even if that person claims to represent a provider.
- Control of the key does not by itself prove the community's identity or authority. Verification should rely on independent organizational evidence and trusted public communications.
- A legitimate verification process should not require disclosure of the secret that protects the account.

Reasoned response: The community should not reply with any credential or code. It should preserve the message if reporting is appropriate, use only established support

channels, and verify any claim independently. Observers can continue checking the public address through the explorer. The private credentials must remain private.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- Wallets can make complex blockchain records and signing functions easier to use.
- Public addresses allow people to receive transfers and inspect account activity without exposing private keys.
- Digital signatures can authorize specific data without publishing the signing secret.
- Seed-based designs can make a connected group of accounts recoverable from one carefully protected backup.
- Public records and private signing authority can support transparency and controlled access at the same time.

IMPORTANT LIMITATIONS AND RISKS

- Loss of a private key or seed phrase may cause permanent loss of access when no recovery service exists.
- Theft or disclosure of a private key or seed phrase may allow unauthorized control.
- A malicious or confusing wallet interface may ask a person to sign harmful data.
- A password may protect a device or application without protecting an exposed seed phrase.
- A public address can reveal transaction patterns and create privacy risks when connected with a person or organization.
- A valid signature proves key control for the signed data, not the signer's complete identity, understanding, or legal authority.
- Recovery methods and compatibility vary among wallets; a phrase or backup may not work as expected in every system.
- Physical damage, malware, phishing, impersonation, coercion, and poor backup practices can defeat otherwise strong cryptography.

COMMON MISCONCEPTIONS

- » "The coins are stored inside the wallet." The blockchain records the assets; the wallet helps manage the credentials and interactions.
- » "A public address and a private key are the same information." The address is intended for public identification; the private key must remain secret.
- » "A public address identifies a person." An address identifies a blockchain destination. Connecting it with a person requires outside evidence.
- » "A wallet password can always recover the account." A password and a seed phrase have different roles, and recovery depends on the wallet design.
- » "A seed phrase is safe because it contains ordinary words." The ordered words may recreate the wallet's keys and must be protected as a powerful secret.
- » "Signing only proves that I logged in." A signature may authorize a transaction, approval, message, or other action.
- » "Support needs my seed phrase to verify or repair the wallet." A legitimate service should never need the seed phrase or private key.
- » "A valid signature proves the signer acted wisely and legally." Cryptography verifies key control and data integrity, not judgment or legal authority.

OFFLINE EXERCISE: PUBLIC, PRIVATE, OR VERIFY FIRST?

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Create three headings on separate paper:

1. May be public in the right context
2. Must remain secret
3. Verify before acting

Place each hypothetical item under the best heading. Some items may require a short explanation.

- » A public BNB Smart Chain address printed on an organization's official information page.
- » A private key displayed by a wallet's export function.
- » A seed phrase written as an ordered list of words.
- » A password used to unlock a wallet application.
- » A temporary authentication code received during login.
- » A public transaction identifier used to locate a record on a blockchain explorer.

- The name of the blockchain network that an address is intended to use.
- A message asking the user to sign data that the user does not understand.
- A screenshot that includes an account balance and public address.
- A request from a supposed support agent for "only the first three words" of a seed phrase.

Then write a short explanation for each question:

- Why can a public address be shared while a private key cannot?
- Why can sharing a public address still create a privacy concern?
- Why should an unexplained signature request be placed under Verify before acting?
- What is the difference between a password and a seed phrase?
- What should a person do if anyone requests a private key, seed phrase, password, or authentication code?

Conclude with four or five sentences describing the personal rules you would use to protect digital credentials.

Important limitation of the exercise: Every item is hypothetical. Do not copy, invent, request, or disclose a real credential, code, account number, or wallet address.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes a blockchain wallet?
   a. A container that physically holds coins and tokens away from the blockchain
   b. A tool that helps a person view blockchain records, manage credentials, and authorize actions
   c. A guarantee that every transaction can be reversed
   d. A public list of every user's private keys
2. Which item must remain secret?
   a. The name of a blockchain network
   b. A public transaction identifier
   c. A private key
   d. A publicly designated receiving address
3. What can a properly verified digital signature help establish?

a. That the signed data was authorized with the corresponding private key and was not altered after signing
b. That the signer made a wise financial decision
c. That the signer owns every asset connected with the address
d. That the signer disclosed the private key to the network

TRUE OR FALSE

» A seed phrase and an application password always perform the same function and can always replace one another.

SHORT EXPLANATION

» In three or four sentences, explain why a public address may support transparency without giving observers authority to move the assets associated with it.

SUMMARY AND PRACTICAL TAKEAWAYS

» Digital assets remain recorded on a blockchain; a wallet helps a person read records, manage credentials, prepare requests, and create signatures.
» A public address identifies a blockchain destination. It does not contain the assets or prove who controls it.
» Public addresses may reveal transaction patterns and should be shared only with attention to network, purpose, and privacy.
» A private key is a secret used to create digital signatures and authorize account actions.
» A signature can prove control of a corresponding key for specific data without revealing the private key.
» A valid signature does not prove wisdom, consent, legal authority, or complete personal identity.
» Some wallets use seed phrases to generate or restore many keys. Not every wallet uses the same method.
» A seed phrase, private key, password, and authentication code have different roles, but all must be protected.
» No legitimate course activity, teacher, support agent, or verification service should request a private key or seed phrase.
» The public Prison Professors community treasury address can support observation through BscScan while its private credentials remain confidential.
» Never place a real credential, code, account number, or wallet address in a course response.

The practical responsibility is to separate information that supports public verification from information that grants private authority.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- Explain what a blockchain wallet does and why the assets are not physically stored inside it.
- Distinguish a public address from a private key.
- Explain how a digital signature can authorize an action without revealing the private key.
- Describe the purpose of a seed phrase and why it may be more sensitive than an ordinary password.
- Use the public treasury example to explain how transparency and confidentiality can work together.
- Identify one benefit, two risks, and one common misconception involving wallets or credentials.
- State the rules you would follow if someone requested a seed phrase, private key, password, authentication code, or unexplained signature.
- Connect careful credential management with responsibility, preparation, judgment, or trust.

Your response should demonstrate your reasoning. Do not create, copy, request, or include any real password, private key, seed phrase, authentication code, account number, wallet address, transaction information, or other sensitive credential.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 12: Wallets, Addresses, Keys, and Seed Phrases, and the date you completed the entry.

Use one of the established Prison Professors Profile methods, subject to your facility's rules:

1. Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 12 — [date completed].

2. Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
3. Send it to an approved family member or supporter who can enter it on 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, transaction details, or other sensitive credentials.