LESSON 13: CUSTODY AND SELF-CUSTODY

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational and Safety Boundary:

> *This lesson provides general education about digital-asset custody, access, recovery, and risk. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, custodian, 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, wallet address, balance, or transaction record in a course response.Opening Guidance*

In Lesson 12, we used the public Prison Professors community treasury as an example of the difference between public observation and private authority. The independent community that organized the PP token made a BNB Smart Chain address visible so people could inspect activity through BscScan. The public record may show what reaches or leaves that address. It does not show who holds the private credentials, how many people must approve an action, or what recovery plan exists.

I have described the treasury arrangement as cold storage. That description is helpful, but it answers only one kind of question. Cold storage generally describes keeping signing credentials away from routine internet-connected use. It does not, by itself, tell us whether one person, several people, or a third-party service has custody. It also does not prove that the backup, approval, or succession plan is adequate.

This lesson adds a second question to the first. Lesson 12 asked what information is public and what information must remain private. Lesson 13 asks who has practical authority to use the private credentials and who carries the responsibility when something goes wrong.

I encourage you to study that question even if your present circumstances do not allow you to create an account or use a wallet. A person can develop judgment before gaining access to technology. Learning how to compare control, convenience, recovery, and risk is part of preparing responsibly.

PURPOSE AND ESSENTIAL QUESTION

Lesson 13 compares third-party custody and self-custody without presenting either approach as universally correct. It explains how different arrangements move control, convenience, recovery duties, and risk among users, organizations, and service providers.

Essential Question:

- How should a careful person weigh convenience, control, recovery, access, counterparty risk, and personal responsibility when evaluating a custody arrangement?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- Define custody, custodian, custodial wallet, self-custody, counterparty risk, and recovery.
- Compare third-party custody and self-custody across control, convenience, access, recovery, and responsibility.
- Explain the useful meaning and important limits of the phrase "not your keys, not your coins."
- Distinguish custody from the separate question of whether a wallet is kept in hot or cold storage.
- Advise hypothetical learners by identifying tradeoffs without prescribing a product or requiring access to technology.

KEY TERMS

CUSTODY

Definition: The practical arrangement for controlling access to an asset or the credentials that can authorize actions involving it. In blockchain systems, custody often turns on who controls the private keys or signing process. Legal definitions may vary by jurisdiction and context.

Sample sentence: The public ledger showed the treasury activity, but it did not reveal the complete custody arrangement.

CUSTODIAN

Definition: A person, company, or service that holds assets or controls access to them on behalf of another person or organization. A custodian may manage private keys, account access, transaction approvals, records, or recovery procedures.

Sample sentence: Before relying on a custodian, the learner wanted to understand how the service protected keys and what would happen if the service failed.

CUSTODIAL WALLET

Definition: A wallet service or account in which a third party controls the private keys or signing authority for the user. The user normally signs in and gives instructions to the provider rather than signing every blockchain transaction with a key the user alone controls.

Sample sentence: The custodial wallet offered password recovery, but the user depended on the provider to honor withdrawal instructions.

SELF-CUSTODY

Definition: An arrangement in which a person or organization directly controls the private keys or other signing credentials. Self-custody reduces dependence on a custodian but places more security, backup, recovery, and operating responsibility on the key holder.

Sample sentence: Self-custody gave the organization direct signing authority and required a careful plan for backup and continuity.

COUNTERPARTY RISK

Definition: The possibility that another person or organization involved in an arrangement will fail, be unable to perform, misuse authority, suffer a security breach, block access, or not honor an agreement.

Sample sentence: A custodial account created counterparty risk because the user depended on the provider to safeguard assets and process valid requests.

RECOVERY

Definition: The process for regaining authorized access after a password, device, key, or other credential is lost, damaged, compromised, or unavailable. Recovery options depend on the custody arrangement and system design.

Sample sentence: The team tested its recovery plan without exposing any real credential or moving an asset.

MAIN LESSON

CUSTODY ASKS WHO CAN AUTHORIZE AN ACTION

Blockchain assets remain recorded on a blockchain. A custody arrangement concerns the authority used to interact with that record. The central question is not who can see a balance. It is who can create or cause the valid signature needed to authorize an action.

That authority can be organized in several ways:

- A user may directly control the key.
- A company may control the key and keep an internal account for the user.
- Several people may need to approve an action together.
- A person and a recovery service may share different parts of the process.
- An organization may use policies, devices, and multiple approvals to divide responsibility.

These arrangements do not all fit perfectly into two boxes. “Custodial” and “self-custodial” are useful starting categories, but real systems may combine elements of both. A careful learner asks exactly who can sign, who can block a request, who can recover access, and what evidence supports the answer.

THIRD-PARTY CUSTODY MOVES KEY CONTROL TO A PROVIDER

In a third-party custody arrangement, a provider controls the keys or signing system. The customer normally has an account with the provider. A username, password, authentication code, identity check, or customer-support process may allow the customer to request an action.

The provider may record many customer balances in its own database. A customer’s balance on the provider’s screen may not correspond to a separate public blockchain address controlled only for that customer. The provider may combine assets, use several wallets, or settle transfers internally. The exact structure depends on the provider and agreement.

Third-party custody may offer useful features:

- Familiar account access.
- Password or account recovery.
- Customer service.
- Security staff and specialized systems.
- Easier coordination for some organizations.
- Procedures for incapacity, death, or a change in authorized personnel.

Those benefits come with dependence. The user must rely on the custodian's security, records, finances, policies, legal compliance, and willingness or ability to process requests. Access may be delayed or limited because of an investigation, technical failure, identity check, account dispute, sanctions screening, court order, provider policy, bankruptcy, or other event.

The word custodian does not guarantee that every provider offers the same legal protections. Insurance, segregation of assets, regulatory status, complaint rights, and bankruptcy treatment can differ. A person should not assume that a crypto account has the same protection as a bank deposit or a traditional securities account. Those questions require current, jurisdiction-specific verification.

SELF-CUSTODY MOVES CONTROL TO THE KEY HOLDER

In self-custody, the user or organization directly controls the keys or signing credentials. No custodian needs to approve an ordinary transaction. This arrangement may give the key holder more direct access and reduce some forms of counterparty risk.

Direct control also creates direct responsibility. A self-custody user may need to:

- Protect private keys and recovery information.
- Maintain trustworthy devices and software.
- Verify networks, addresses, and transaction details.
- Create backups that are both secure and usable.
- Plan for loss, theft, damage, incapacity, or death.
- Avoid phishing, malicious applications, and false support requests.
- Understand that a valid signature may be difficult or impossible to reverse.

A provider may not be able to reset a lost private key. If the only usable credentials disappear, access may disappear with them. If an attacker obtains the credentials, the attacker may be able to sign actions that the network treats as valid.

Self-custody therefore removes one kind of dependency while increasing operational responsibility. It does not remove blockchain risk, software risk, smart-contract risk, device risk, physical risk, coercion, human error, or legal obligations.

HOT AND COLD DESCRIBE CONNECTION, NOT CUSTODY

People often combine two different comparisons:

- Hot or cold generally describes whether signing credentials are available to an internet-connected system during ordinary use.
- Custodial or self-custodial describes who controls the keys or signing authority.

A self-custody wallet may be hot or cold. A custodian may also use hot wallets for routine operations and cold storage for longer-term protection. Calling a wallet "cold" does not prove that it is self-custodial, well backed up, or governed responsibly. Calling a wallet "hot" does not prove that a third party controls it.

The Prison Professors community treasury helps make this distinction practical. When I describe the treasury as cold storage, I am describing how the signing credentials are kept relative to online use. The public BNB Smart Chain record does not disclose the full custody design, backup plan, number of authorized people, or internal approval rules. Those controls should not be published casually, but responsible stewards should still document and test them privately.

"NOT YOUR KEYS, NOT YOUR COINS" IS A WARNING

The phrase "not your keys, not your coins" reminds people that an account balance shown by a provider is not the same as direct control of a blockchain key. If the provider controls the keys, the user depends on that provider to recognize the account and carry out valid requests.

That warning is useful, but it has limits.

First, controlling a key does not automatically prove legal ownership. A key holder may be an employee, trustee, agent, custodian, thief, or unauthorized person. Outside records and agreements may determine who is entitled to the asset.

Second, direct control does not guarantee good security. A person can lose a seed phrase, approve a harmful transaction, use compromised software, or fail to make a recovery plan.

Third, some people or organizations may reasonably value recovery support, shared controls, recordkeeping, or legal safeguards more than sole key control. A carefully evaluated custodian may fit some needs, while self-custody may fit others.

Fourth, the word "coins" can hide technical and legal complexity. A user may hold a contractual claim against a provider rather than direct control over a specific on-chain unit. The agreement, provider records, blockchain record, and applicable law may each answer a different question.

A more complete principle is: know who controls the keys, know what rights the records and agreement provide, know how recovery works, and know which risks remain.

RECOVERY CHANGES WITH THE CUSTODY ARRANGEMENT

In a custodial account, recovery may resemble recovery for another online service. The provider might reset a password after identity verification. That convenience depends on the provider's procedures and continued operation. A criminal who defeats the recovery process may also gain access.

In self-custody, recovery may depend on a seed phrase, backup, secondary device, shared-signature arrangement, or another technical design. No customer-service representative may be able to restore access. A backup must be protected from theft while remaining available after loss or damage.

Recovery should be planned before a crisis. A sound plan asks:

- What event would require recovery?
- Which credential or person would restore access?
- How is unauthorized recovery prevented?
- What happens if one authorized person is unavailable?
- Can the process be tested without revealing a real secret or moving real assets?
- How will the plan change when a person's living situation, device access, health, or legal circumstances change?

This course will never ask a learner to design a real recovery scheme or disclose a credential. The purpose is to develop the questions that responsible planning requires.

PERSONAL CIRCUMSTANCES AND INSTITUTIONAL RULES CAN CHANGE THE ANSWER

Custody is not only a technical choice. A person may lack reliable device access, a safe place for a backup, acceptable identification, or permission to use an account. An incarcerated learner may be prohibited from possessing a device, creating a financial account, receiving authentication messages, or using a digital-asset service.

Those limitations are not a failure to learn. The learner can still compare arrangements, recognize unsafe claims, build vocabulary, and prepare for future decisions. No activity in this course requires violating a facility rule, opening an account, asking another person to act as a substitute account holder, or handling an asset.

Using another person's account can create additional problems involving ownership, taxes, access, consent, reporting, and trust. A family member should not create or control an account merely to complete a course activity. Learning can remain fully offline.

ORGANIZATIONS NEED CONTINUITY AND ACCOUNTABILITY

An organization faces questions that differ from those of an individual. If only one person can authorize treasury activity, illness, loss, departure, coercion, or misconduct may create a single point of failure. If too many people can act independently, accountability may weaken.

A responsible organizational process may consider:

- Written authority and purpose.
- Separation of duties.
- More than one approval for important actions.
- Limits on transaction size or frequency.
- Independent record review.
- Backup and succession.
- Incident response.
- Periodic testing and revision.

These controls can exist in custodial, self-custodial, or shared arrangements. Technology cannot replace governance. A public address may support transparency, but it does not explain whether internal authority is appropriate or whether every transfer followed the mission.

APPLIED SCENARIO: WHAT THE TREASURY ADDRESS CANNOT PROVE

The independent PP token community sends community-generated fees to a public treasury address associated with the Prison Professors mission. Observers can use BscScan to inspect the public ledger. I have said that the resources are intended to remain visible while being reserved in the treasury for a stated period. This example is educational and does not promote the token or any digital asset.

Imagine that a new volunteer sees the address and says:

Claim: “Because the address is public and the funds are described as cold storage, BscScan proves that the treasury is completely safe, that Prison Professors alone controls it, and that the funds can always be recovered.”

The claim goes beyond the evidence.

- BscScan may show activity connected with the address. It does not show the private keys.
- A cold-storage description does not identify every person or system with signing authority.

- A public balance does not prove legal ownership, mission compliance, or the terms of an outside agreement.
- The explorer does not show whether recovery information exists, whether it is accurate, or whether authorized people can use it.
- The explorer does not reveal internal approval limits, succession plans, or security practices.
- A visible balance at one moment does not guarantee future value, access, or safety.

Reasoned response: The public record supports a limited kind of transparency. It can help observers verify on-chain activity associated with the published address. A complete custody assessment would require additional evidence about authority, safeguards, recovery, governance, and applicable agreements. Sensitive credentials should remain private even while organizational policies and accountability standards are documented.

The lesson for a participant is broader than Web3. Credibility grows when a person distinguishes what the evidence proves from what the evidence does not prove. That habit strengthens critical thinking and responsible communication.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF THIRD-PARTY CUSTODY

- Familiar account access and support may reduce some technical burdens.
- A provider may offer password recovery, identity verification, monitoring, and specialized security.
- Organizations may gain recordkeeping, role management, or continuity features.
- Some regulated arrangements may provide safeguards that do not exist in an informal self-custody setup, although protections vary and must be verified.

IMPORTANT THIRD-PARTY CUSTODY RISKS

- The provider may be hacked, become insolvent, misuse assets, make recordkeeping errors, or stop operating.
- Access may be delayed, restricted, or denied.
- The provider may combine customer assets or use them in ways the user did not understand.
- Fees, withdrawal limits, supported networks, privacy practices, and recovery rules may change.

» A login balance may depend on the provider's internal records rather than direct user control of a specific on-chain address.

POSSIBLE BENEFITS OF SELF-CUSTODY

» The key holder can authorize actions without asking a custodian.
» Direct key control can reduce dependence on a provider's solvency, availability, or withdrawal policy.
» The user or organization can design its own approval, storage, and recovery process.
» Public blockchain activity can be inspected without requiring a custodian's account statement.

IMPORTANT SELF-CUSTODY RISKS

» Lost or destroyed credentials may cause permanent loss of access.
» Stolen credentials may allow unauthorized transfers.
» A harmful signature, wrong address, wrong network, or malicious application may cause an irreversible loss.
» Backups may be exposed, damaged, forgotten, or unavailable during an emergency.
» One person may become a single point of failure.
» Direct control may create responsibilities the user does not have the tools, permission, or experience to manage safely.

COMMON MISCONCEPTIONS

» "Self-custody is always safer." It removes some custodian risks but adds key-management, device, backup, and human risks.
» "A custodian removes all responsibility from the user." The user still must protect login credentials, evaluate the provider, review records, and understand the agreement.
» "Cold storage means self-custody." Cold storage concerns connection and use; either a user or a custodian may control the keys.
» "If I control the key, the law must treat me as the owner." Key control is technical evidence, not a complete legal conclusion.
» "If a provider can reset my password, it can always recover my assets." Recovery depends on the provider, account status, records, security process, and continued operation.

» "A public treasury address proves the full custody arrangement." A public address shows ledger activity, not private authority, recovery, or governance.
» "Using a family member's account solves an access problem." It may create additional ownership, tax, consent, reporting, security, and trust problems.
» "Not your keys, not your coins ends the discussion." The phrase identifies an important dependency but does not compare every right, safeguard, or operational risk.

OFFLINE EXERCISE: ADVISE WITHOUT PRESCRIBING

Estimated time: 25–30 minutes

Materials: Separate paper and a pencil.

Draw six headings across the top of a page or use six labeled sections:

1. Control
2. Convenience
3. Recovery
4. Access
5. Counterparty risk
6. Personal responsibility

Read each hypothetical learner profile. For each one:

» Identify the person's most important needs and constraints.
» Explain one possible benefit of third-party custody.
» Explain one possible risk of third-party custody.
» Explain one possible benefit of self-custody.
» Explain one possible risk of self-custody.
» Identify information that is missing.
» State a careful next question without recommending a product or telling the person to buy, transfer, or hold an asset.

PROFILE A: LIMITED ACCESS

Jordan is incarcerated. Facility rules do not permit a personal smartphone, wallet, financial account, or authentication device. Jordan wants to understand Web3 and prepare for future decisions.

PROFILE B: RECOVERY PRIORITY

Renee has reliable internet access but does not have a safe, stable place to store a physical backup. She values a recovery process and is concerned about forgetting credentials.

PROFILE C: DIRECT CONTROL

Luis has technical experience, secure device access, and time to maintain backups. He wants direct signing authority but has not made a plan for illness or incapacity.

PROFILE D: MISSION TREASURY

A small nonprofit receives digital assets for a mission. One director currently controls the only usable signing credential. The board wants transparency, continuity, and protection against one person acting alone.

Conclude with a paragraph explaining why the same custody arrangement may be reasonable for one situation and inappropriate for another.

Important limitation of the exercise: Every profile is hypothetical. Do not create an account, ask another person to create one, copy a real service's terms, disclose a credential, or handle an asset. The correct work is the comparison and reasoning.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes third-party custody?
   a. The user alone controls every private key and no provider can affect access
   b. A provider controls the keys or signing process and the user depends on the provider to carry out authorized requests
   c. The blockchain automatically guarantees reimbursement for every loss
   d. A public address reveals every internal approval rule
2. Which statement correctly distinguishes cold storage from self-custody?
   a. Cold storage always means that one individual controls the keys
   b. Self-custody always requires an internet-connected wallet
   c. Cold storage concerns how credentials are kept relative to online use, while self-custody concerns who controls them
   d. The two terms always mean exactly the same thing

3. What is counterparty risk?
    a. The possibility that another party may fail, misuse authority, block access, or not honor an agreement
    b. The guarantee that a provider will recover every lost credential
    c. The process of reading a public address on a blockchain explorer
    d. The mathematical creation of a public key

TRUE OR FALSE

» Controlling a private key automatically proves legal ownership, wise judgment, and a complete recovery plan.

SHORT EXPLANATION

» In three or four sentences, explain why "not your keys, not your coins" is a useful warning but not a complete custody analysis.

SUMMARY AND PRACTICAL TAKEAWAYS

» Custody concerns who controls access to the credentials or process that can authorize an action.
» In third-party custody, a provider controls the keys or signing system and the user depends on the provider.
» In self-custody, the user or organization controls the keys and accepts greater security, backup, and recovery responsibility.
» Third-party custody may offer convenience and recovery support while creating counterparty risk.
» Self-custody may reduce provider dependence while increasing operational and personal risk.
» Hot and cold storage describe connection and use; custodial and self-custodial describe control.
» "Not your keys, not your coins" identifies a real dependency but does not settle questions of legal rights, safety, recovery, or suitability.
» A public address can support transparency without revealing the full custody, governance, or recovery arrangement.
» Institutional rules and personal circumstances may limit available choices. Learning does not require opening an account or violating a rule.
» Responsible organizations combine technology with written authority, review, continuity, and human accountability.

» Never include a real credential, account number, wallet address, balance, or transaction detail in a course response.

The practical responsibility is to understand where control sits, what recovery requires, which other parties must be trusted, and which risks remain after the arrangement is chosen.

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:

» Define custody in your own words.
» Compare a custodial wallet with self-custody.
» Explain how control, convenience, recovery, access, counterparty risk, and responsibility change between the two.
» Explain the difference between cold storage and self-custody.
» Discuss what the phrase "not your keys, not your coins" helps a learner remember and what it leaves unexplained.
» Use the public Prison Professors community treasury example to distinguish observable blockchain evidence from private custody and governance information.
» Identify one circumstance in which a person may reasonably value third-party recovery support and one circumstance in which direct key control may matter.
» Explain how institutional rules or present circumstances can limit action without limiting learning.
» Connect careful custody analysis with responsibility, preparation, judgment, or trust.

Your response should demonstrate reasoning. Do not create, copy, request, or include any real password, private key, seed phrase, authentication code, account number, wallet address, balance, 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 13: Custody and Self-Custody, 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 13 — [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, balances, transaction details, or other sensitive credentials.