

UNDERSTANDING WEB3**PREFACE: PREPARING TODAY FOR SUCCESS TOMORROW**

A Prison Professors Self-Directed Course

A PERSONAL NOTE FROM ME TO YOU

If you are working through this course in a prison, you may be studying without an instructor and with limited access to books, technology, or people who can answer your questions. I understand the frustration that can come from those conditions. I also know that meaningful learning can begin with a printed lesson, a pen, and a decision to use time deliberately.

My name is Michael Santos. I am the founder of Prison Professors, a nonprofit organization that provides educational resources to people in prison. I created Prison Professors to share lessons that leaders taught me while I served 26 years in federal prison. Those lessons helped me prepare for release, build trust, create opportunities, and become financially independent.

After reaching financial independence, I devoted the rest of my life to this mission. I want to show people in prison how they can use time today to prepare for success tomorrow. I cannot promise that a course will produce a job, an income stream, a sentence reduction, or a particular institutional decision. I can promise that disciplined learning and a documented record of preparation can give other people more evidence to consider when they evaluate you.

I began my journey with introspection and questions. I studied people who had built lives of meaning and contribution. Then I compared the decisions they made with the decisions that had brought me to prison. I understood that the system would not change on my behalf. If I wanted a different future, I had to change the way I thought and acted.

I read, wrote, reflected, and kept records of what I learned. I tried to connect each lesson with a decision I could make. Over time, those small choices became a body of work. I shared much of that journey in *Earning Freedom: Conquering a 45-Year Term*, which is part of our curriculum at Prison Professors.

The work I completed while serving my sentence helped people see more than my conviction and prison record. They could evaluate the goals I set, the books I studied, the projects I completed, and the commitments I kept. Some people began to

trust me before they ever met me. Their trust created relationships and opportunities that helped me build several income streams after release.

Your path will be your own. Still, you can begin using the same process: learn, think, write, document, and improve. We want every member of our community to become a Prison Professor. Write your own curriculum and show how you are using time today to prepare for higher levels of success tomorrow.

WHY I FOUNDED PRISON PROFESSORS

People in prison do not have access to the same learning resources that exist in society. Internet access may be restricted or unavailable. A person may not be able to watch a video, join an online class, or practice with a digital tool. Lockdowns, transfers, work assignments, health problems, and other conditions may interrupt a study plan.

Prison Professors exists to help close that gap. We create self-directed courses that people can use in print and offline. We provide those resources without charging the government or the people completing the courses. A participant does not need to purchase anything to learn from the self-directed courses we offer.

Our work rests on a simple belief. When people invest time and effort in themselves, they can develop knowledge, judgment, communication skills, and confidence. When they memorialize what they learn by writing, they create evidence of their commitment to personal development. That record can help them prepare for employment, entrepreneurship, community service, and lawful income opportunities.

No document guarantees an outcome. Yet a strong record can strengthen conversations with family members, mentors, employers, program staff, and other decision-makers. We believe that greater preparation can help families build stability and can contribute to reducing intergenerational cycles of poverty and recidivism.

THE THREE PROMISES I MAKE

I make three promises to every member of the Prison Professors community.

1. I WILL ALWAYS BE TRUTHFUL.

» If I do not know an answer, I will not pretend that I do.

2. I WILL NEVER ASK YOU TO DO ANYTHING THAT I DID NOT DO.

» I pursued self-directed learning while serving my sentence. I wrote about what I learned. I documented goals, progress, setbacks, and revised plans. I



reached out to people and invited them to evaluate my work. The exercises in this course follow that same discipline.

3. YOU WILL NEVER PAY PRISON PROFESSORS FOR THE RESOURCES WE PROVIDE.

- » We do not charge participants or government agencies for these educational resources. Supporters who believe in the mission help us continue. Their support allows us to distribute courses and encourage people who are preparing for law-abiding, contributing lives.
- » These promises create accountability for me. I encourage you to create promises for yourself as well. A personal code can guide decisions when motivation is low, circumstances change, or no instructor is present.

EDUCATION CAN BEGIN FROM WHERE YOU ARE

Some participants have enjoyed school for years. Others may have left school early, struggled with reading, lost confidence, or spent more time surviving than studying. If education has not been part of your history, you do not need to hide from that history. You can start from your present position.

Self-directed learning does not require you to know everything before you begin. It requires you to take responsibility for the next step. You can read one section. You can circle an unfamiliar term. You can write a question in the margin. You can explain an idea in your own words. You can complete one dated response and then return for the next lesson.

Progress may feel slow at first in this course on Web3. Technical words such as blockchain, wallet, token, smart contract, and decentralization may be unfamiliar. The lessons define those words and use examples to build understanding. If a paragraph is difficult, read it again. Break it into smaller parts. Use the vocabulary section. Write what you think the passage means before checking another explanation.

The purpose is not to memorize every definition. The purpose is to strengthen the way you learn, question claims, compare choices, identify risks, and communicate your reasoning. Those abilities can transfer to many fields, including fields that do not use Web3.

YOUR PROFILE CAN BECOME AN ASSET

At Prison Professors, we established the Profiles component so that any participant can build a public or shareable record of preparation. A Profile gives you a place to show more than a criminal charge or a sentence. It can show how you are using time, what you are learning, how your thinking is changing, and what you intend to contribute.

YOUR PROFILE MAY INCLUDE:

- » A biography that explains the experiences, values, and decisions that shaped you.
- » Journal entries that record what you learned and how you intend to apply it.
- » Book reports that show reading comprehension, reflection, and communication.
- » Release plans that identify goals, resources, risks, responsibilities, and measurable steps.
- » Course responses and completed projects that demonstrate sustained self-directed learning.

A Profile becomes more credible when it contains specific, dated work. Instead of writing only, “I want to improve,” you can identify what you studied, the insight you gained, the choice you will make, and the date when you will review your progress. Over time, those entries can show consistency, growth, and follow-through.

That record can become an asset for self-advocacy. You may use it to help family members, mentors, employers, program staff, or decision-makers understand your preparation. It may support a lawful request for greater responsibility, a new opportunity, or a higher level of liberty. The authority to grant any request belongs to the appropriate decision-maker, and a Profile does not guarantee relief. It gives you a stronger way to present evidence of your work.

Prison Professors will promote participants who work consistently to develop their Profiles. Our goal is to help the broader community find and evaluate your discipline through your writing.

WHY I CHOSE WEB3

Web3 is an evolving area of the digital economy. It includes blockchains, digital assets, smart contracts, decentralized applications, and new ways for people to coordinate online. Some projects are useful. Some are experimental. Some are poorly designed or dishonest. Prices can be volatile, transactions may be irreversible, and legal or regulatory requirements can change.

I did not create this course to promote speculation or encourage you to buy a token. You can complete every lesson without internet access, an account, a wallet, a digital asset, a purchase, or a transaction. I created it to help you understand a technology that may influence future work, commerce, recordkeeping, and communities.

The course also includes a real example connected with Prison Professors. CZ is the founder of Binance. We became friends as he went through his own experience with

the justice system. I helped him work on his biography, *Freedom of Money*, and I narrated the audiobook. In the book, CZ wrote about his support for Prison Professors.

After the book was published, people whom neither CZ nor I knew organized an independent Web3 community with a token created in support of our nonprofit mission. Neither CZ nor I created the token. Prison Professors did not organize, manage, or control the token project. The community website identifies the effort as independent, not as an official Prison Professors product or endorsement.

The independent community used BNB Smart Chain, a public blockchain, and programmed transaction fees that send resources to a public treasury address supporting our nonprofit mission. A blockchain explorer allows anyone to view activity associated with a public address. In Lesson 9, we explain how the BscScan explorer displays that public record.

A screenshot supplied for this course on July 21, 2026, showed the public treasury address holding more than 943 wrapped BNB, or WBNB, along with a smaller native BNB balance. The approximate market value shown at that time exceeded \$500,000. The balance can change as transactions occur, and the dollar estimate can rise or fall with the market price of BNB.

I share this case as an educational example, not as a recommendation to acquire or promote any asset. The case shows how people who did not know me personally learned about documented work, formed a community, used Web3 tools, and chose to support a mission. That experience reinforces a lesson I learned in prison: when you prepare consistently and make your work visible, people may discover your record and decide to help.

Future lessons return to this case to explain how tokens, public addresses, custody, transactions, smart contracts, decentralized finance, and governance interact. I encourage you to evaluate the case with the same questions you would apply to any project. What can you verify? Who controls each part? Which risks remain? Which claims are observations, and which are predictions?

HOW I ENCOURAGE YOU TO USE THIS COURSE

I encourage participants to work through the sequence in order. Each lesson builds upon the previous lesson. You do not need to finish quickly. A steady routine will help you retain more than a rushed reading.

READ BEFORE ANSWERING.

Read the entire lesson before writing your final response. Mark unfamiliar terms and return to the definitions. If your circumstances allow, explain the central idea aloud or in writing as if you were teaching another person.

WRITE YOUR OWN RESPONSE FIRST.

At the end of each lesson, answer the questions in your own words. Use complete sentences. Include examples from the lesson and, when appropriate, connect the concept with your life, goals, or observations. Record the date. Those entries can show that you are self-directed and striving to reach a higher potential.

The printed workbook does not include writing space. Use separate paper and keep your responses together when possible. A simple heading can identify the course, lesson number, lesson title, and date.

COMPARE ONLY AFTER YOU FINISH.

An appendix will include sample responses written as I would answer them. Do not begin with those responses. Complete your own work first. Then compare your reasoning with the sample.

The sample is not the only acceptable answer. Use it to identify an idea you missed, a risk you should consider, or a clearer way to explain your conclusion. If the comparison changes your thinking, write a short revision. That revision becomes evidence that you can receive information, reflect, and improve.

ADD THE WORK TO YOUR PROFILE.

If you want to extend the exercise, record your strongest responses as dated journal entries on your Prison Professors Profile. If email is available, send the response to Playbook@PrisonProfessors.org. Put the date you completed the journal entry in the subject line and identify the Web3 lesson.

If you do not have email access, you may send the response through a family member who can upload it, or mail it to:

Prison Professors 1205 BMC Drive, Suite 706 Cedar Park, TX 78613

Follow all facility rules for correspondence. Do not include passwords, private keys, seed phrases, authentication codes, account credentials, or other sensitive information in a response.

BUILD A PATTERN.

One response may show effort on one day. A series of dated responses can show a pattern of self-directed learning. Add book reports, journal entries, release-plan updates, and other projects when you can. Review older work and notice where your writing, judgment, and goals have improved.

MY INVITATION TO YOU

I know that confinement can limit your choices. It can also create long periods when the future feels distant. I cannot choose your circumstances or promise how another person will respond to your work. I can encourage you to control the choices that remain available.

You can choose to learn. You can choose to write. You can choose to document a plan. You can choose to revise after receiving new information. You can choose to build a record that shows who you are becoming.

That process worked for me. It helped me turn years in prison into years of preparation. It helped me earn trust, build relationships, create lawful income streams, and devote my life to helping others prepare.

I invite you to begin this course with the same spirit. Do not wait until every resource is available. Start with the lesson in front of you. Complete the work in your own voice. Date it. Preserve it. Then take the next step.

Your past will always be part of your story. Every day gives you an opportunity to write a new chapter. A documented record cannot erase a conviction or guarantee an outcome. It can show your preparation as you respond to collateral consequences: the legal, social, and practical barriers that can follow a conviction.

Develop your curriculum. Become your own Prison Professor.

Michael Santos,

Founder, Prison Professors

UNDERSTANDING WEB3

LESSON 1: BECOMING YOUR OWN PRISON PROFESSOR

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This course provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this lesson.

OPENING GUIDANCE

While serving 26 years in federal prison, I realized that if I wanted a better life after release, I would have to pursue a self-directed learning path. The world was changing, but I could not depend on classrooms, teachers, or access to evolving technology. I had to learn by reading, developing a vocabulary, asking questions, and practicing how to communicate.

In essence, I had to create a curriculum that would help me overcome the obstacles I expected to face. The lessons I learned through that process helped me grow. I may introduce the ideas in this course as a Prison Professor, but my goal is for you to become your own prison professor. You can build a personal curriculum, develop useful skills, and document the work you are doing to prepare for the future.

This course does not ask you to accept every claim about Web3. It asks you to learn the language, understand the basic systems, recognize risks, compare alternatives, and explain your conclusions. That is how knowledge becomes judgment.

PURPOSE AND ESSENTIAL QUESTION

Lesson 1 introduces the purpose, structure, learning method, and boundaries of Understanding Web3. It also explains how your reading, reflection, and writing can create evidence of sustained preparation.

Essential Question:

- » How can I use this course to strengthen my judgment, develop useful learning habits, and document the preparation I am making for the future?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Describe the purpose and six-section structure of the course.
- » Distinguish technology education from financial, investment, legal, or tax advice.
- » Explain how reading, reflection, and journal writing can document preparation.
- » Identify learning habits that support critical thinking and self-directed study.
- » State a personal reason for studying Web3 without relying on promises or promotional claims.

KEY TERMS

SELF-DIRECTED LEARNING

Definition: A learning process in which a person takes active responsibility for setting goals, using available resources, monitoring progress, and evaluating understanding.

Sample sentence: My self-directed learning plan includes reading carefully, defining new terms, and reviewing what I wrote.

CRITICAL THINKING

Definition: The disciplined practice of asking questions, examining evidence, recognizing assumptions, and reaching a reasoned conclusion.

Sample sentence: Critical thinking helped the learner separate a verified fact from an exciting prediction.

DIGITAL ECONOMY

Definition: Economic activity that depends on or is significantly shaped by digital technologies, services, infrastructure, and data.

Sample sentence: Online communication, electronic payments, digital records, and remote work are parts of the digital economy.

PROFILE

Definition: In this course, a Prison Professors record that may include dated journal entries documenting a participant's learning, preparation, goals, and growth.



Sample sentence: She added a journal entry to her Profile to document what she learned and how she evaluated the lesson.

PREPARATION

Definition: Deliberate action taken before an opportunity, responsibility, or challenge arises.

Sample sentence: Completing each lesson and explaining it in his own words became evidence of preparation.

MAIN LESSON

WHY THIS COURSE BEGINS WITH LEARNING

You may expect a Web3 course to begin with cryptocurrency, blockchain, or technical vocabulary. Those subjects are coming. First, however, we need to establish how you will learn.

Web3 can be difficult to study because the subject combines technology, finance, business, law, and social organization. People also use the term in different ways. Some explain it carefully. Others use it to advertise products, predict the future, or create excitement. If you begin by memorizing slogans, you may repeat words without understanding what they mean. If you begin with a sound learning method, you can examine unfamiliar claims without being controlled by them.

The method in this course is simple: read, define, question, apply, write, and re-view. None of those actions requires a smartphone or an account. Each one can be completed with a printed lesson, separate paper, and a pencil. Access to technology may expand your resources, but limited access does not prevent serious learning.

BECOMING YOUR OWN PRISON PROFESSOR

Becoming your own prison professor means accepting responsibility for your education while using whatever lawful resources are available. It does not mean pretending that you already know the answers. It does not mean rejecting teachers, feedback, or expertise. It means that you do not wait passively for ideal conditions before you begin preparing.

During my years in prison, I could not control the sentence, the schedule, or the technology available to me. I could control whether I read, whether I thought about what I read, and whether I practiced communicating what I learned. Those repeated choices helped me build skills that remained useful when circumstances changed.

Your circumstances may be different from mine. Your goals may also be different. The principle remains useful: identify what you can control and act on it consistently. You may control when you read, how you organize notes, whether you define unfamiliar words, how honestly you evaluate your understanding, and whether you complete the journal entry. Small actions repeated across 20 lessons can create a meaningful record.

Self-directed learning is not the same as learning alone. A book can guide you. A facilitator can offer feedback. A family member can encourage you. A knowledgeable person can correct an error. The learner's responsibility is to use support thoughtfully rather than surrendering judgment. A serious learner can say, "I do not understand this yet," and then decide what question to ask next.

HOW THE 20 LESSONS ARE ORGANIZED

The course contains six sections that build from foundations toward responsible application.

1. Understanding the Internet and Web3 introduces changes in the internet, the idea of Web3, and the tradeoffs between centralized and decentralized systems.
2. Blockchain Foundations explains shared ledgers, transactions, blocks, hashes, networks, consensus, and blockchain layers.
3. Digital Assets and Tokenization distinguishes cryptocurrencies, tokens, stablecoins, non-fungible tokens, and tokenized assets.
4. Wallets, Transactions, Custody, and Safety explains how people interact with blockchain systems and why security, privacy, and careful verification matter.
5. Smart Contracts, Applications, Finance, and Governance introduces programmable agreements and the applications, risks, and decision-making systems built around them.
6. Applications, Skills, Careers, and Responsible Participation connects technical understanding to ethical judgment, transferable skills, continuing education, and future preparation.

I encourage participants to work through the sequence in order. Each lesson will build upon the previous lesson. Later lessons will depend on words and ideas introduced earlier. You are not expected to master every detail on the first reading. Your responsibility is to build an accurate foundation and notice where your understanding needs work.

USE A REPEATABLE LEARNING CYCLE

Each lesson follows a recurring cycle.

1. Read: Move slowly enough to identify the main idea and supporting details.
2. Define: Study the vocabulary and use each important word in context.
3. Question: Ask what evidence supports a claim, what may be missing, and what alternatives exist.
4. Apply: Complete a scenario, comparison, exercise, or paper simulation.
5. Write: Explain the concept in your own words and connect it to responsible preparation.
6. Review: Check your reasoning, identify errors, and decide what needs further study.

This cycle turns reading into active work. A person may look at every page and still learn very little. Active reading requires decisions. You may underline a definition, place a question mark beside an unclear sentence, summarize a paragraph in a few words, or list a benefit beside a limitation. The physical mark is not the goal. The goal is to make your thinking visible so you can examine it.

VOCABULARY CREATES ACCESS

Specialized words can create barriers. They can also become tools. When you learn a term such as blockchain, wallet, or smart contract, you gain the ability to understand a discussion that may once have seemed closed to you.

Vocabulary should improve communication, not create a performance. Using a complicated word does not prove understanding. You should be able to define a term plainly, use it in a sentence, recognize an incorrect use, and explain how it connects with other ideas. If you cannot do those things yet, return to the definition and example.

This course introduces a small group of terms in each lesson. Keep a personal vocabulary list if your circumstances permit. Write the date, the term, a short definition, and your own sentence. Over time, the list will show growth that may be difficult to notice from one day to the next.

CRITICAL THINKING IN A NOISY SUBJECT

Critical thinking does not mean criticizing everything. It means evaluating a claim before deciding how much confidence to place in it. A careful learner asks questions such as:

- » Who made this claim, and what does that person or organization want me to believe or do?
- » What evidence supports the claim?
- » Is the statement a fact, an opinion, a forecast, or a promotion?



- » What assumptions does the statement depend upon?
- » What are the possible benefits, limitations, costs, and risks?
- » What simpler alternative should be considered?
- » What information would change my conclusion?

These questions are especially important in Web3. A description may explain a real capability while leaving out cost, complexity, concentration of power, privacy concerns, security failures, or legal uncertainty. Another description may focus only on problems and ignore useful experiments. Your responsibility is not to become automatically enthusiastic or automatically hostile. Your responsibility is to develop a reasoned position based on the best information available.

WEB3 IS ONLY ONE PART OF THE DIGITAL ECONOMY

The digital economy includes many activities shaped by digital technology and data. Online marketplaces, digital records, remote services, software, electronic communication, and digital payments are examples. Web3 is one part of that broader environment. It does not represent every digital activity, and it does not replace every useful system that came before it.

Studying Web3 can still be valuable even if you never purchase a digital asset or use a blockchain application. The subject can help you practice evaluating technical claims, comparing systems, recognizing security risks, and communicating about change. Those abilities can transfer to many forms of learning and work.

The course does not promise that Web3 will create a job, income, investment return, or opportunity for any particular participant. Technology changes. Organizations change. Laws and markets change. Durable preparation comes from developing skills that remain useful when a prediction turns out to be wrong.

DOCUMENTING PREPARATION THROUGH YOUR PROFILE

At the end of every lesson, you will receive prompts for a Profile journal entry. The purpose is not to produce a perfect essay. The purpose is to create a dated record of thought, effort, and improvement.

A strong entry does more than repeat definitions. It explains an idea, applies it, identifies a limitation, and connects the lesson to a responsible choice or future goal. Over time, the entries can demonstrate that you followed a structured course, practiced writing, considered risks, and sustained a self-directed learning process.

A Profile is evidence of preparation, not a guarantee. A journal entry cannot promise employment, support, release, or success. It can help you show what you chose



to do with your time and how your thinking developed. That record becomes stronger when your writing is specific, honest, organized, and in your own words.

Protect your privacy while documenting your work. Never include passwords, account numbers, authentication codes, private keys, seed phrases, or other sensitive credentials. You also do not need to disclose private financial information or details that could create a personal safety risk. Thoughtful writing can be meaningful without revealing everything about your life.

COURSE BOUNDARIES PROTECT YOUR JUDGMENT

Education explains concepts and helps you ask better questions. Advice tells a specific person what action to take based on that person's circumstances. This course provides education. It does not tell you to buy, sell, hold, borrow, invest, create an account, open a wallet, or use a financial product.

The course also does not provide individualized legal or tax guidance. Rules can depend on jurisdiction, facility policy, personal circumstances, and changes over time. If a real decision requires professional advice, the lesson cannot replace an appropriately qualified adviser.

These boundaries do not weaken the course. They strengthen it by keeping the focus on understanding and judgment. You can study how a wallet works without opening one. You can evaluate a token claim without purchasing anything. You can compare a blockchain with an ordinary database without deciding that either one is always better.

YOUR REASON FOR STUDYING MATTERS

A clear reason can help you continue when the material becomes difficult. Your reason does not need to sound impressive. You may want to understand language you hear in the news. You may want to communicate more effectively with family members or future colleagues. You may want to strengthen your research and writing. You may want to evaluate technology claims more carefully or prepare for a changing workplace.

Avoid building your reason around fear of missing out or a promise of quick wealth. Those motives can encourage rushed decisions and weak judgment. A durable reason focuses on what you can develop: knowledge, discipline, communication, ethical awareness, and evidence of preparation.

At the end of this lesson, you will create a learning commitment. It is not a contract with Prison Professors. It is a statement to yourself about how you intend to approach the work. You may need to adjust the schedule when circumstances change. The important measure is whether you return to the process and continue.

APPLIED SCENARIO: TWO WAYS TO COMPLETE A LESSON

Two learners receive the same printed lesson.

The first learner reads quickly, copies several sentences into a journal entry, and finishes. The response uses technical words but does not explain them. When asked what evidence supports a claim, the learner cannot answer.

The second learner reads more slowly. This learner circles unfamiliar terms, writes plain definitions, identifies one claim that needs evidence, completes the exercise, and explains a conclusion in original words. The response is not perfect, but it shows reasoning and identifies what remains unclear.

Both learners turned in a response. Only the second response provides strong evidence of self-directed learning.

Reasoned conclusion: Completion matters, but the quality of the learning process matters more. A useful Profile entry shows how the learner interpreted, questioned, applied, and evaluated the material. It does not merely prove that the learner reached the last page.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF THE COURSE METHOD

- » A repeatable process can make unfamiliar material more manageable.
- » Vocabulary practice can improve reading and communication.
- » Scenarios and exercises can reveal gaps that passive reading may hide.
- » Dated journal entries can document sustained effort and developing judgment.
- » Offline design allows meaningful participation without an account or internet access.

IMPORTANT LIMITATIONS AND RISKS

- » A self-directed course cannot answer every question or replace all expert guidance.
- » A learner can misunderstand a concept and repeat the error without careful review or feedback.
- » Technical information can become outdated, especially when it concerns particular networks, laws, or markets.
- » Promotional language may look educational while encouraging a financial action.



- » A Profile entry can create privacy risks if it includes sensitive personal or account information.
- » Course completion does not establish professional expertise or guarantee an opportunity.

COMMON MISCONCEPTIONS

- » “Self-directed learning means I must learn alone.” You remain responsible for your learning, but appropriate guidance, correction, and support can improve it.
- » “Longer writing always proves deeper thinking.” Clear reasoning and relevant examples matter more than unnecessary length.
- » “Finishing the course will make me a Web3 expert.” The course provides an introductory foundation and a method for continued learning.
- » “I must buy cryptocurrency to understand Web3.” Every required activity can be completed without purchasing an asset or creating an account.
- » “A Profile guarantees that someone will support me.” A Profile can document preparation, but other people and institutions make their own decisions.

ETHICAL LEARNING

Ethical learning requires honesty. Use your own words. Identify uncertainty instead of pretending to know. Credit important sources when appropriate. Do not copy another person’s experience and present it as your own. Respect privacy, facility rules, intellectual property, and the safety boundaries of the course.

OFFLINE EXERCISE: MY 20-LESSON LEARNING COMMITMENT

Estimated time: 15–20 minutes

Materials: Separate paper and a pen or pencil.

Write a one-page learning commitment using the steps below. This is a planning exercise, not the Profile journal assignment.

1. Write one or two honest reasons why you want to study Web3.
2. Identify two abilities you want to strengthen, such as reading, vocabulary, writing, critical thinking, digital safety, or decision-making.
3. Choose a realistic study routine. State when or how often you intend to read, complete exercises, and write journal entries.
4. Identify one likely obstacle, such as interruptions, limited materials, difficult vocabulary, or discouragement.
5. Write one response you can use when that obstacle appears.



6. List two rules for protecting your judgment. Examples include checking the source of a claim, comparing benefits with risks, or refusing to act because of pressure or fear of missing out.
7. List two rules for protecting your privacy. Do not write any real credential or account information.
8. Finish this sentence: Across these 20 lessons, I intend to demonstrate that I can...
9. Date the commitment and keep it with your course materials when circumstances permit.

After every five lessons, reread the commitment. Mark what is working and what needs adjustment. Revising a plan is not a failure. It is part of directing your learning responsibly.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which action best demonstrates self-directed learning?
 - a. Repeating a promotional slogan without examining it
 - b. Waiting for perfect conditions before beginning
 - c. Setting a goal, using available resources, checking understanding, and adjusting the plan
 - d. Assuming that completing a page proves mastery
2. Which statement accurately describes a boundary of this course?
 - a. It recommends particular digital assets for each participant.
 - b. It provides general technology education rather than individualized financial, legal, or tax advice.
 - c. It requires every participant to create a wallet.
 - d. It guarantees employment after completion.
3. Which example provides the strongest evidence of preparation?
 - a. A dated journal entry that explains an idea, evaluates a limitation, and applies the lesson
 - b. A copied definition with no explanation
 - c. A claim that the learner already understands everything
 - d. A list of assets the learner hopes will increase in price



TRUE OR FALSE

- » Completing all 20 lessons and creating a Profile guarantees that an employer, court, institution, or supporter will provide an opportunity.

SHORT EXPLANATION

- » In two or three sentences, identify one learning habit you intend to use and explain how it can strengthen your critical thinking or preparation.

SUMMARY AND PRACTICAL TAKEAWAYS

- » The course contains 20 lessons organized into six sections.
- » Self-directed learning requires active responsibility, not isolation or pretending to know everything.
- » A useful learning cycle is to read, define, question, apply, write, and review.
- » Critical thinking weighs evidence, assumptions, benefits, limitations, risks, and alternatives.
- » Web3 is one part of the broader digital economy.
- » The course provides education, not individualized financial, investment, legal, or tax advice.
- » Profile journal entries can document sustained preparation, but they do not guarantee an outcome.
- » No required activity involves purchasing an asset, opening an account, or using the internet.

The practical goal is not to sound like an expert. It is to become a more disciplined learner who can explain what you know, identify what you do not know, and continue preparing responsibly.

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 why you chose to study Web3 and what you hope to understand.
- » Identify two learning or communication skills you intend to strengthen.
- » Describe the study habits you will use across the 20 lessons.
- » Explain what you want your completed Profile entries to demonstrate about your preparation.

- » Identify one important course boundary and explain why it protects your judgment.
- » End with one commitment you can control, even if your circumstances or access to technology remain limited.

Your response should be honest and specific, but you do not need to disclose private financial, legal, medical, family, or facility information. You are not being asked to support Web3, oppose it, purchase anything, or predict its future.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 1: Becoming Your Own Prison Professor, 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 1 — [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 in your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, or other sensitive credentials.



UNDERSTANDING WEB3

LESSON 2: HOW THE INTERNET CHANGED: FROM THE EARLY WEB TO WEB2

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This course provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, platform, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this lesson.

OPENING GUIDANCE

Before we study Web3, I encourage participants to understand the changes that came before it. New technology rarely appears all at once. People build upon earlier systems, respond to limitations, and develop new ways to communicate or conduct business.

At the time authorities arrested me on August 11, 1987, the World Wide Web did not yet exist. The internet already existed in technical and research settings, but it had not yet become the public resource that most people recognize today. I learned about its development from inside prison by reading.

Readers of my book, *Earning Freedom: Conquering a 45-Year Prison Term*, will understand how strongly I believe in self-directed study. While serving my sentence, I could not use the internet or depend on direct access to computers and web platforms. Still, I could study how the world was changing. I read, defined unfamiliar terms, asked questions, and connected what I learned to the life I wanted to build after release.

That learning supported practical preparation. As the internet and the economy changed, I studied the opportunities those changes were creating. Self-directed learning helped me develop and follow a savings plan while I was in prison. The savings I accumulated became one of the resources that helped me establish myself after release.

Learning from a distance did not give me the same experience as using the technology. It did, however, allow me to develop a vocabulary, ask better questions, and prepare before access became available. Participants can use the same method. You do not need access to a computer or the internet to understand how the internet developed or to examine the tradeoffs that came with its growth.

This lesson uses the labels early web and Web2. Those labels are helpful, but they are not official software versions or exact periods on a calendar. They describe broad patterns. As you read, focus on the movement from a web centered mainly on publishing and reading pages toward a web where large numbers of people could create content, interact, and conduct activities through online platforms.

PURPOSE AND ESSENTIAL QUESTION

Lesson 2 explains how the internet developed from an environment centered largely on reading published information into one that supports widespread participation, sharing, collaboration, and commerce through online platforms. It also examines the opportunities and tradeoffs created when centralized services organize those activities.

Essential Question:

- » How did the movement from the early web to Web2 expand what people could do online, and how did it change who controlled the services, rules, and data?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Describe important differences between the early web and Web2.
- » Explain how platforms and user-generated content changed online participation.
- » Identify benefits and tradeoffs associated with centralized online services.
- » Explain why labels such as early web and Web2 describe overlapping patterns rather than exact dates.

KEY TERMS

INTERNET

Definition: A worldwide system of connected computer networks that exchange information by following shared technical rules.

Sample sentence: The internet provides the underlying connections that allow many services, including the World Wide Web and email, to operate.

EARLY WEB

Definition: A broad label for the first period of the World Wide Web, when many websites primarily published linked pages for visitors to read.

Sample sentence: An early-web site might provide a fixed collection of articles that only the site owner could update.



WEB2

Definition: A broad label for the more participatory web, where people commonly create accounts, contribute content, interact with others, and use online services as platforms.

Sample sentence: Posting a review, sharing a video, or selling through an online marketplace reflects common Web2 patterns.

PLATFORM

Definition: A digital service that organizes interactions among different users, such as creators and viewers, buyers and sellers, or drivers and riders.

Sample sentence: The marketplace platform connects sellers with buyers and establishes rules for their interactions.

USER-GENERATED CONTENT

Definition: Material created and contributed by people who use an online service, including posts, comments, reviews, photographs, audio, and videos.

Sample sentence: Customer reviews are user-generated content that may help other people evaluate a product.

CENTRALIZED SERVICE

Definition: A service managed by one organization or governing authority that controls its main systems, policies, accounts, and access decisions.

Sample sentence: A centralized service may operate computers in many locations while one company still controls the rules and user accounts.

MAIN LESSON

BEGIN BY SEPARATING THE INTERNET FROM THE WEB

People often use the words internet and web as if they mean the same thing. They are connected, but they are not identical.

The internet is the broader network infrastructure. It allows connected computers and networks to exchange information through shared technical rules. Many services can operate through that infrastructure. Email is one example. File transfers, messaging, online games, video calls, and the World Wide Web are others.

The web is a system of linked resources that people reach through web addresses and browsers. A web page may contain text, images, sound, video, forms, or interactive tools. When you select a link, the browser requests another resource and displays it.

A transportation comparison may help. Roads provide infrastructure that many vehicles can use. A delivery service is one activity that operates on those roads. In a similar way, the internet provides connections, and the web is one major system that uses them. The comparison is limited because digital networks do not function exactly like roads, but it helps separate the foundation from one service built upon it.

HOW THE WORLD WIDE WEB BEGAN

The internet existed before the web. In 1989, Tim Berners-Lee proposed the World Wide Web while working at CERN, a scientific research organization. The project was designed to help researchers share and connect information. He developed core elements that included web addresses, a transfer method, a page-formatting language, a server, and a browser-editor. CERN states that the first website described the Web project itself.

In 1993, CERN placed the Web software in the public domain and later made an open-licence release available. That decision allowed other people and organizations to use and build upon the technology. Open standards also helped different computers, browsers, and websites work together rather than requiring every visitor to use one company's private system.

Many early websites resembled digital documents, directories, or brochures. A university might publish research information. A news organization might post articles. A business might provide its address, hours, and product descriptions. A person with the necessary knowledge might create a personal page. Visitors generally followed links and read what the publisher made available.

This description is a pattern, not an absolute rule. Early internet users communicated through email, discussion groups, and other interactive systems. Some early websites also accepted forms or visitor contributions. The phrase early web helps us describe what was common; it does not mean every person could only read or that all sites worked in the same way.

FROM PUBLISHING PAGES TO PARTICIPATING THROUGH SERVICES

Over time, creating and using online services became easier. Faster connections, improved browsers, databases, mobile devices, and simpler publishing tools supported richer interaction. A person no longer needed to build an entire website to contribute something publicly. A service could provide the forms, storage, search tools, audience, and rules.

People began creating profiles, publishing blogs, posting comments, sharing photographs and videos, rating products, editing shared pages, and communicating through social networks. Businesses could offer online shopping, payment tools, advertising, customer reviews, and services that matched one group of users with another.

User-generated content became a central part of this environment. The service operator supplied the platform, but participants supplied much of the material and activity. A video-sharing service became more useful when people uploaded videos. A marketplace became more useful when sellers offered goods and buyers provided ratings. A social network became more useful when friends, families, organizations, and creators joined and contributed.

This growth can reinforce itself. When more people use a service, the service may become more valuable to other users. Economists call this a network effect. Network effects can help a useful platform expand quickly, but they can also make it difficult for a smaller alternative to attract enough participants.

WHAT THE LABEL WEB2 DESCRIBES

The term Web2 became widely used during the early 2000s. In a 2005 explanation, technology publisher Tim O'Reilly described Web2 through patterns such as the web functioning as a platform and a movement from publishing toward participation. He also warned that the term did not have a hard boundary and could become an unclear marketing label.

Web2 was not a single invention, official upgrade, or date when every website changed. No central authority replaced “Web1” with “Web2.” Older and newer patterns existed together. They still do. A modern website may publish fixed pages with no account or comment feature. An older online community may have allowed participation long before people commonly used the label Web2.

For this course, Web2 is a useful shorthand for several related developments:

- » More people could create and share content without building a website.
- » Online services became interactive and responsive.
- » Platforms organized communication, commerce, entertainment, and work.
- » Accounts allowed services to remember activity and personalize experiences.
- » Large service providers stored data and established rules for participation.
- » Advertising, subscriptions, fees, and data-supported business models financed many services.

These features do not appear in every Web2 service, and they do not make a service automatically beneficial or harmful. They give us criteria for comparison.

HOW A PLATFORM ORGANIZES PARTICIPATION

A platform does more than display information. It creates an environment where different people or groups can interact. An online marketplace may connect buyers and sellers. A social service may connect creators, viewers, and advertisers. A work platform may connect clients and service providers.

The platform operator usually provides important benefits. It may maintain the technology, search and organize information, reduce some transaction costs, enforce safety rules, remove harmful material, update security, process disputes, and help participants find one another. A well-run centralized service can make a complicated activity easier and more reliable.

Centralized does not mean that one physical computer performs every task. A large service may use thousands of machines and facilities in many locations. The service is centralized in the governance sense: one organization has primary authority over the accounts, software, policies, and stored information.

That authority creates responsibility and power. The operator may decide who can create an account, what content is permitted, how search results or recommendations are ordered, what fees apply, which data are collected, and whether an account or post will be restricted. Some control is necessary to operate a service. The important question is how that control is used, explained, and reviewed.

BENEFITS THAT EXPANDED OPPORTUNITY

Web2 services lowered barriers to participation for many people. A creator could reach an audience without owning printing equipment or a broadcast station. A small business could display products, accept orders, and communicate with customers. Families could share updates across long distances. Learners could find communities, publish questions, and collaborate on documents. Employers and workers could discover one another through online listings and professional networks.

Centralized platforms can also provide convenience. One account may allow a person to store information, return to earlier work, communicate with many users, and use consistent tools. A central operator can correct software, respond to attacks, back up information, and apply common policies across the service.

These benefits are real, but access is not equal. A person may lack a reliable connection, a suitable device, permission to create an account, a payment method, digital skills, or confidence that personal information will be protected. A service that expands opportunity for one participant may remain unavailable to another.



TRADEOFFS INVOLVING DATA, RULES, AND DEPENDENCE

Participation through a platform often requires accepting the platform's structure. The operator may store posts, contacts, purchases, searches, location information, or other activity. Some services use data to improve functions, detect abuse, personalize content, or support advertising. Those uses can create value, but they can also create privacy and security risks.

A platform may change its rules, prices, recommendations, or available features. It may remove content or close an account correctly, incorrectly, or without an explanation the participant considers adequate. If a person has built an audience, reputation, collection of work, or source of income inside one service, leaving may be difficult. Contacts may not move easily, and another service may not have the same users.

The Federal Trade Commission reported in 2024 that major social media and video-streaming companies collected and used extensive personal information, including for advertising and automated systems, while providing users limited control in important areas. That finding concerns particular services and practices; it does not mean every centralized platform handles data in the same way. It does show why participants should examine what information a service collects, how the business earns revenue, and what choices users actually have.

Critical thinking requires us to hold two ideas together. A platform can create genuine opportunity and convenience. The same platform can also concentrate authority, collect sensitive information, and create dependence. Responsible evaluation considers both sides and asks whether alternatives exist.

HOW THIS HISTORY PREPARES US TO STUDY WEB3

Web3 developed partly in response to questions raised during the Web2 era. Could people interact online without depending as heavily on one platform operator? Could they control certain digital assets or credentials more directly? Could shared rules be enforced through a distributed network?

Those questions do not prove that a Web3 approach is better. Decentralized systems introduce their own costs, risks, complexity, governance problems, and forms of concentration. Web2 services will also continue to evolve. The purpose of learning this history is to understand the problem before evaluating a proposed solution.

In Lesson 3, we will examine what people mean by Web3. I encourage participants to carry forward three questions: Who provides the service? Who makes the rules? Who controls the data or digital record?

APPLIED SCENARIO: A COMMUNITY EDUCATOR CHOOSES AN ONLINE APPROACH

A community educator wants to share short employment-readiness lessons and allow participants to discuss them.

Under an early-web pattern, the educator creates a website with a page for each lesson. Visitors can read the material by following links. The educator controls what is published and updates the pages. This approach can be simple and predictable, but participants have no built-in way to post responses. Adding interactive features may require additional technical work.

Under a Web2 pattern, the educator opens a group on a large platform. The platform provides accounts, posting tools, comments, notifications, search, and an existing audience. Participants can contribute questions and examples. The educator can begin without building the full technical system.

The convenience comes with tradeoffs. The platform establishes the account rules, stores participant activity, decides how posts are displayed, and may change features or restrict access. Some learners may not be permitted or able to create accounts. The educator may also have difficulty preserving the complete learning record outside the service.

Reasoned conclusion: Neither approach is automatically correct. The educator should compare audience access, participation needs, privacy, recordkeeping, cost, technical skill, and dependence on the service provider. A combined approach might publish the lessons on an accessible website while offering optional discussion through a separate service. The choice should follow the learning goal rather than a technology label.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF WEB2 PATTERNS

- » People can publish, communicate, and collaborate without building an entire technical system.
- » Platforms can connect participants who would otherwise have difficulty finding one another.
- » Reviews, comments, and shared knowledge can help communities solve problems.
- » Central operators can maintain infrastructure, apply policies, and respond to security problems.
- » Online marketplaces and work platforms can create new ways to reach customers or opportunities.

IMPORTANT LIMITATIONS AND RISKS

- » An account, compatible device, reliable connection, or payment method may be required.
- » The service operator may collect significant data and control how it is used.
- » A change in rules, fees, rankings, or access can affect participants who depend on the service.
- » Popularity and engagement systems may reward attention rather than accuracy or public value.
- » Network effects can concentrate users and influence in a small number of services.
- » User-generated content may include errors, manipulation, harassment, fraud, or unlawful material.

COMMON MISCONCEPTIONS

- » “The early web had no interaction.” Interactive services existed, but publishing and reading fixed pages were more prominent web patterns.
- » “Web2 began on one exact date.” The label describes overlapping changes that developed over time.
- » “Centralized means one computer.” A centralized service can use many distributed machines while one organization controls the service.
- » “User-generated content belongs to the user in every sense.” A participant may create the content while platform terms and applicable law affect storage, use, removal, and rights.
- » “A free service has no cost.” A service may be funded through advertising, fees charged to another group, data-supported business models, or other sources.
- » “Web2 is obsolete because Web3 exists.” Web2 patterns remain widespread, and newer systems often depend on ordinary web technologies and centralized services.

ETHICAL PARTICIPATION

Participation does not remove personal responsibility. A person should communicate honestly, respect privacy and intellectual property, evaluate sources, follow lawful rules, and avoid spreading material merely because it attracts attention. Never post another person’s private information or sensitive credentials. When a service makes participation easy, slow down long enough to consider who may be affected by what you share.

OFFLINE EXERCISE: SORT THE INTERNET ACTIVITIES

Estimated time: 15–20 minutes

Materials: Separate paper and a pen or pencil.

Draw three columns and label them Early-web pattern, Web2 pattern, and Could fit both. Place each activity below into one column. Then write one sentence explaining each item you placed in Could fit both.

1. Reading a university page that only the university can update.
2. Posting a product review through a personal account.
3. Viewing a fixed page containing a business's address and hours.
4. Uploading a video and receiving comments from viewers.
5. Following links through an online collection of public documents.
6. Buying an item through a marketplace that connects many sellers and buyers.
7. Reading a news article on a website.
8. Adding information to a shared community page.
9. Sending a message through an online service.
10. Publishing a personal page that visitors can read.
11. Searching a directory of websites.
12. Joining a work platform that matches clients with service providers.

When you finish, review your choices. Items 7, 9, 10, and 11 may reasonably fit more than one column depending on how the service works. For each ambiguous item, identify the feature that influenced your decision. Ask whether participants merely receive information or can also create content, maintain accounts, interact, and rely on a platform to organize the activity.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes the relationship between the internet and the World Wide Web?
 - a. They are two names for exactly the same system.
 - b. The web is one major service that operates through the broader internet.
 - c. The internet was created after Web2.
 - d. The web only includes social-media platforms.
2. Which activity most clearly reflects a Web2 pattern?



- a. Reading a fixed page that only its publisher can update
 - b. Following a link from one document to another
 - c. Creating an account, uploading a video, and responding to comments
 - d. Printing an online article for later study
3. Which statement accurately describes a centralized online service?
- a. It must operate from one physical computer.
 - b. It cannot contain user-generated content.
 - c. One organization has primary authority over the service's accounts, rules, and systems.
 - d. It gives every user equal power to change the service's policies.

TRUE OR FALSE

- » Web2 began on one official date when every website received the same technical upgrade.

SHORT EXPLANATION

- » In two or three sentences, identify one benefit and one tradeoff of using a centralized platform for communication, learning, or business.

SUMMARY AND PRACTICAL TAKEAWAYS

- » The internet is the broader network infrastructure; the web is one major system that uses it.
- » The early web commonly emphasized publishing linked pages for visitors to read.
- » Web2 describes a more participatory environment built around accounts, platforms, interaction, and user-generated content.
- » Early-web and Web2 patterns overlap. They are not separated by one exact date.
- » Platforms can lower barriers, connect participants, organize information, and support commerce or collaboration.
- » Centralized service operators also control important rules, accounts, systems, and data practices.
- » User participation can create value while also introducing privacy, accuracy, safety, and dependence concerns.
- » Understanding Web2 helps us evaluate why people proposed Web3 approaches and what problems those approaches claim to address.



The practical goal is to compare systems without reducing history to slogans. Ask what people can do, what the service provider contributes, what the participant gives up, and what alternatives remain available.

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:

- » Describe one way internet services changed communication, learning, work, or business.
- » Explain how user-generated content can create value for a community or platform.
- » Identify one benefit of a centralized online service and one tradeoff involving control, privacy, access, or dependence.
- » Explain why the labels early web and Web2 should not be treated as exact dates or rigid categories.
- » Connect this history to one skill you want to strengthen, such as evaluating sources, protecting privacy, communicating responsibly, or comparing alternatives.
- » End with one question about control or ownership that you want Lesson 3 to help you answer.

Your response should be honest and specific, but you do not need to disclose private account, financial, legal, medical, family, or facility information. You are not being asked to create an account, use an online platform, purchase anything, or support one model of the internet over another.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 2: How the Internet Changed: From the Early Web to Web2, 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 2 — [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 in your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, or other sensitive credentials.



UNDERSTANDING WEB3

LESSON 3: WHAT IS WEB3?

A Prison Professors Self-Directed Course

Estimated time: 70–105 minutes

Educational Boundary:

This course provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, platform, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this lesson.

OPENING GUIDANCE

In the previous lesson, I described how I studied changes to the internet while I remained in prison. I could not gain direct experience with the technology, but I could read, build a vocabulary, ask questions, and prepare. That self-directed approach helped me distinguish what I knew from what I still needed to learn.

I encourage participants to use the same discipline with Web3. The term appears in technical writing, business proposals, news reports, and advertisements. Different people may use it to mean different things. Some describe working systems. Others describe goals that developers hope to reach. Still others use Web3 as a promotional label.

We do not have to praise or reject a technology before we understand it. We can begin with clear definitions and careful questions. We can ask what the system does today, who controls each part, what responsibility falls on the participant, and what evidence supports a claim.

This lesson provides a working definition. Later lessons will explain the individual technologies in greater depth. For now, the goal is to understand the main ideas commonly associated with Web3 and to practice separating an established capability from an aspiration or sales message.

PURPOSE AND ESSENTIAL QUESTION

Lesson 3 introduces Web3 as a group of technologies and ideas involving blockchain networks, digital assets, programmable agreements, and new approaches to control or ownership. It also explains why Web3 is a proposed direction for parts of the internet rather than a complete replacement for Web2.

Essential Question:

- » What does Web3 mean, and how can a careful learner distinguish what the technology can do from what someone hopes or claims it will do?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define Web3 without relying on promotional language.
- » Identify major technologies and ideas commonly associated with Web3.
- » Distinguish an established capability from an aspiration, opinion, forecast, or promotional claim.
- » Explain why Web3 does not replace every useful Web2 service.

KEY TERMS

WEB3

Definition: A broad and still-developing term for technologies and ideas that use decentralized networks, blockchains, digital assets, and programmable rules to give participants new ways to interact with data, value, applications, or one another.

Sample sentence: The learner treated Web3 as a collection of developing approaches rather than one finished product.

DIGITAL OWNERSHIP

Definition: Control over a digital asset or record based on the rules of a system, often demonstrated through possession of a private key or another recognized form of authorization.

Sample sentence: Digital ownership may allow a person to transfer a token, but it does not automatically include copyright or control over every related file.

PEER-TO-PEER

Definition: A way for participants in a network to interact directly or as equals under shared rules rather than routing every action through one central operator.

Sample sentence: The peer-to-peer network allowed participants to exchange messages without one computer controlling every connection.



PROTOCOL

Definition: A set of technical rules that allows computers or network participants to communicate and coordinate.

Sample sentence: A shared protocol tells separate computers how to format, send, and interpret information.

PERMISSIONLESS

Definition: Open to participation under the system's rules without requiring advance approval from a central administrator.

Sample sentence: A permissionless network may let a person create an address without asking one company to approve an account.

INTEROPERABILITY

Definition: The ability of different systems, applications, or networks to exchange information or work together through compatible rules and standards.

Sample sentence: Interoperability can allow a digital credential to be recognized by more than one compatible service.

MAIN LESSON

BEGIN WITH A WORKING DEFINITION

Web3 does not name one company, network, application, or official upgrade to the World Wide Web. It is an umbrella term. People use it for a developing set of technologies and design goals that seek to change how some online services store information, enforce rules, represent assets, and distribute control.

The National Institute of Standards and Technology, known as NIST, describes Web3 as a proposed vision that would shift parts of the internet from an organization-centered structure toward a more user-centered structure. In that vision, users would have greater control over data and digital assets, while decentralized or distributed systems would perform some work now handled by central service providers.

The word proposed is important. Some Web3 components already operate. Public blockchains record transactions. Digital tokens represent different forms of value or access. Smart contracts—programs stored and executed on a blockchain—apply programmed rules. Decentralized applications use these components to offer services.

The broader vision is not fully achieved. A service may use a blockchain while depending on a company for its website, customer support, data storage, software

updates, or access to outside information. Participation may also require internet access, suitable equipment, technical skill, transaction fees, and careful protection of credentials. A responsible definition must include both the working technology and the unfinished goals.

For this course, we will use the following working definition: Web3 is a broad set of developing technologies and ideas that use blockchain networks, digital assets, programmable rules, and decentralized designs to give participants new ways to interact with data, value, applications, and one another.

This definition does not claim that every Web3 project is decentralized, useful, safe, or successful. It gives us a starting point for investigation.

WHY PEOPLE PROPOSED WEB3 APPROACHES

Lesson 2 examined how Web2 platforms made it easier for people to publish, communicate, build audiences, and conduct business. Those benefits often depend on an organization that controls accounts, software, policies, and stored information.

Web3 proposals ask whether some activities can follow shared protocols instead. A protocol is a set of rules that separate computers or participants can follow. The ordinary web already depends on protocols and standards. They help different browsers, servers, and devices exchange information.

Web3 extends the protocol idea into areas such as shared recordkeeping, digital assets, programmable transactions, identity, and organizational decision-making. Instead of asking one company to maintain the only official record, participants may rely on a network that follows agreed rules. Instead of receiving permission to open an account from a platform, a participant may create a blockchain address and interact under the protocol's conditions.

Supporters often connect these designs to goals such as greater user control, portability, open participation, and resistance to a single operator's failure or policy change. Those are goals to evaluate, not guaranteed outcomes. The design of the network, the distribution of power, the quality of the software, and the participant's ability to use it safely all matter.

THE COMMON BUILDING BLOCKS

Many Web3 services combine several parts.

A blockchain network maintains a shared record according to its protocol. Computers called nodes may store, verify, or help update that record. Lessons 5 through 8

will explain how blocks, transactions, cryptography, consensus, and network layers support this work.

A digital asset is something represented in digital form that a system recognizes as having a holder, status, or set of rules. In Web3, tokens may represent units of a cryptocurrency, access rights, voting power, a claim associated with another asset, or a unique digital item. The token is a record governed by the network and its software. Its existence does not guarantee that it has financial value, legal rights, usefulness, or a trustworthy issuer.

A smart contract is a program that runs on a blockchain. It can receive a transaction, examine conditions, update records, or transfer tokens according to its code. The word contract can be misleading. A smart contract is computer code; whether it also creates an enforceable legal agreement depends on facts and applicable law. Code can execute consistently and still contain a mistake, insecure design, or unfair rule.

A decentralized application, often shortened to dapp, connects a user interface with one or more smart contracts or decentralized services. The visible website may look much like a Web2 application. Some parts can be decentralized while others remain under the control of a developer, company, hosting provider, or small group. The label dapp should lead to questions about architecture, not an assumption that every part lacks a central operator.

A wallet is software or hardware that helps a person manage cryptographic keys and authorize actions. Depending on the design, the participant or a service provider may control the keys. Greater direct control can reduce dependence on an account provider, but it can also place more security and recovery responsibility on the participant. Never share a private key, seed phrase, password, or authentication code.

WHAT DIGITAL OWNERSHIP CAN AND CANNOT MEAN

In a Web2 service, an operator often maintains the account and the official database. A participant may purchase or earn a digital item, but the service decides how that item can be used. If the account closes or the service ends, access may disappear.

Some Web3 systems allow a person to control a blockchain-recorded asset through a private key. The person may be able to transfer the asset to another compatible address without asking the original application to edit its private database. That is an established technical capability in many blockchain systems.

The phrase digital ownership still requires careful interpretation. Control of a token does not automatically grant copyright in an image, ownership of a physical object, a guaranteed market, or access to every related service. Those rights depend on the

token's code, the issuer's promises, platform rules, contracts, and applicable law. If an outside organization must honor the token, the participant still depends on that organization.

Ownership also brings responsibility. If a person controls an asset through a key and loses that key, there may be no central office able to restore access. If a scammer obtains the key or persuades the person to approve a harmful transaction, the network may carry out the instruction exactly as submitted. Control and protection cannot be separated.

PEER-TO-PEER AND PERMISSIONLESS DO NOT MEAN RULE-FREE

In a peer-to-peer system, participants can communicate or exchange under shared rules without requiring one central operator to approve each action. The network and protocol still perform important coordinating work. Software verifies messages, records actions, and rejects requests that do not follow the rules.

Similarly, permissionless does not mean that every person can do anything. It generally means that the base network does not require advance approval from one administrator before a participant can use the protocol. The participant must still meet technical conditions, pay required fees, follow applicable law, and have the necessary access and knowledge.

Other layers may impose permission. A website can block a location. A company can restrict its interface. A wallet provider can decide which features to offer. A government can regulate conduct. A small group may control software updates or important resources. When someone calls a service permissionless, ask which layer is open and which layers still have gatekeepers.

INTEROPERABILITY IS A GOAL THAT REQUIRES REAL WORK

Interoperability means that different systems can exchange information or work together through compatible rules. A portable credential, for example, is useful only if other systems can read it, verify it, and understand what it represents.

Public standards can support interoperability. The World Wide Web Consortium has developed standards for decentralized identifiers and other web technologies. Its work demonstrates an important principle: interoperability depends on agreed formats, testing, governance, and implementation. A project cannot become interoperable merely by using the word.

Blockchain networks also have different rules, data structures, security designs, and assets. Moving information or value between them may require an exchange

service, bridge, shared standard, or other connecting system. Those connections introduce their own risks. A claim that something “works everywhere” needs evidence about which systems support it and what happens when one part fails.

SEPARATE CAPABILITY FROM ASPIRATION AND PROMOTION

A capability is something a system can demonstrate under stated conditions. “This public blockchain records token transfers” describes a testable capability. A limitation may still apply, but the statement can be checked.

An aspiration describes a desired future. “Users will control all of their online data” expresses a goal. It may guide development, but it is not proof that current services have achieved it.

An opinion expresses a judgment. “This design is fairer than every centralized service” depends on values, evidence, and comparison criteria.

A forecast predicts what may happen. “Most websites will use this protocol within five years” concerns an uncertain future.

A promotional statement is written to attract attention, participation, or money. Words such as revolutionary, guaranteed, effortless, risk-free, and once-in-a-lifetime should increase scrutiny. A promotional statement may contain some facts, but its purpose and missing information matter.

When evaluating a claim, ask: What exactly is being promised? What evidence can be checked? Under what conditions does the feature work? Who controls the parts that are not decentralized? What costs, risks, and responsibilities are left out?

WEB3 WILL NOT REPLACE EVERY USEFUL WEB2 SERVICE

Web3 and Web2 are not sealed boxes. A Web3 application normally uses internet connections, web pages, software interfaces, and other technologies that developed during earlier periods. It may also use centralized services for speed, storage, customer support, identity checks, or recovery.

Centralized services can be appropriate when one accountable organization must correct errors, protect sensitive records, provide assistance, or update a system quickly. A distributed design may be useful when several parties need a shared record and do not want one participant to control it. Neither design wins every comparison.

The responsible question is not, “Is Web3 better than Web2?” Ask, “What problem are we trying to solve, which design fits that problem, and what tradeoffs follow?” Lesson 4 will deepen that comparison by examining centralization and decentralization directly.

APPLIED SCENARIO: A PORTABLE TRAINING CREDENTIAL

A nonprofit training organization wants graduates to show employers that they completed a workforce-development program. Its proposal says:

- » Completion records will be represented by digital credentials that learners can present to compatible employers.
- » The credential system will use a public standard so more than one compatible application can verify a record.
- » No graduate will ever lose access, and every employer in the country will accept the credential.
- » The program will revolutionize hiring and eliminate unfair employment decisions.

The first two statements describe planned technical features that can be tested. A reviewer should still ask who issues the credential, what information becomes public, how errors are corrected, which applications are compatible, and what happens if a key is lost.

The third statement makes a forecast and an absolute promise. A technical design cannot force every employer to participate or guarantee that no person will lose access. The fourth is promotional. A credential may improve how a learner presents verified accomplishments, but it cannot by itself eliminate every source of unfairness.

The nonprofit should also consider whether a blockchain is necessary. A standards-based digital credential might work with centralized, federated, or decentralized systems. The organization should compare privacy, portability, cost, security, correction procedures, accessibility, and employer acceptance before selecting the technology.

Reasoned conclusion: The proposal contains a potentially useful idea, but the strongest promises go beyond the evidence. A careful learner separates the verifiable feature from the hoped-for social result.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF WEB3 APPROACHES

- » Shared protocols may reduce dependence on one service provider for certain records or transactions.
- » Participants may control and transfer some digital assets directly through cryptographic authorization.
- » Public networks can allow new applications to use an existing shared record or program.



- » Open standards may support portability and interoperability among compatible systems.
- » Programmable rules can coordinate actions among parties that do not rely on the same central database.

IMPORTANT LIMITATIONS AND RISKS

- » A system may describe itself as decentralized while control remains concentrated among developers, token holders, infrastructure providers, or interface operators.
- » Direct control can increase responsibility for security, key storage, transaction review, and recovery.
- » Public blockchain records may create privacy problems because information can be visible and difficult to remove.
- » Smart contracts and connecting systems may contain bugs or security weaknesses.
- » Fees, network congestion, device requirements, internet access, and technical complexity can limit participation.
- » Tokens can be volatile, illiquid, unnecessary, misleadingly promoted, or connected to fraud.
- » Rules and legal treatment vary by activity and jurisdiction and may change over time.

COMMON MISCONCEPTIONS

- » “Web3 has one official definition.” The term covers several technologies and goals, and credible sources describe it in different ways.
- » “Web3 is a completed third version of the web.” Many components work today, but the wider user-controlled vision remains developing.
- » “Blockchain means the entire service is decentralized.” Websites, governance, data sources, and development can remain centralized.
- » “Permissionless means there are no rules.” Participants must follow the protocol, and other layers or laws may restrict conduct.
- » “Owning a token means owning every related right.” Copyright, physical ownership, access, and legal claims require separate analysis.
- » “Interoperability happens automatically.” Systems need compatible standards, testing, governance, and safe connections.
- » “Web3 makes Web2 obsolete.” The approaches overlap, and many useful services will continue to use centralized or mixed designs.

ETHICAL PARTICIPATION

Responsible participation begins with honesty. Do not describe an aspiration as a completed result or a risky activity as guaranteed. Do not use technical language to pressure someone who lacks information. Respect privacy, intellectual property, lawful rules, and the limits of your own knowledge.

Never share or request a private key, seed phrase, password, or authentication code. Question unsolicited offers, promises of guaranteed returns, urgent demands, impersonation, and anyone claiming that payment will recover lost digital assets. Learning about Web3 does not require buying, transferring, or holding an asset.

OFFLINE EXERCISE: CLASSIFY THE CLAIMS

Estimated time: 20–25 minutes

Materials: Separate paper and a pen or pencil.

Create four headings: Fact or testable capability, Opinion, Forecast or aspiration, and Promotional statement. Place each claim under the heading that best describes it. Then choose four claims and write one question that would help you evaluate each one.

1. This blockchain recorded the transaction at a specific time and address.
2. A smart contract can update a blockchain record when its programmed conditions are met.
3. A user-controlled internet is fairer than every company-operated service.
4. Within five years, most employers will accept blockchain-based credentials.
5. This token is the opportunity of a lifetime.
6. A permissionless network does not require one central administrator to approve every participant at the protocol layer.
7. Every Web3 application protects privacy better than every Web2 application.
8. The service plans to let participants present a credential through more than one compatible application.
9. This revolutionary project will eliminate fraud.
10. Control of a token does not automatically establish copyright in a related image.
11. People will eventually own and manage all of their personal data online.
12. The application uses a blockchain, so no person or organization controls any part of it.

Some claims may combine more than one category. If you see a mixed claim, identify the part that can be tested and the part that expresses judgment, prediction, or promotion. Explain your reasoning. The quality of your explanation matters more than guessing a label.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best defines Web3 for this course?
 - a. One finished product that replaced Web2 on a specific date
 - b. A broad set of developing technologies and ideas involving block-chains, digital assets, programmable rules, and decentralized designs
 - c. Any website that accepts an online payment
 - d. A guarantee that users control every part of an internet service
2. Which statement describes an established technical capability rather than an aspiration or promotion?
 - a. This public blockchain records token transfers according to its protocol.
 - b. Web3 will make every online service fair.
 - c. This token is guaranteed to change your life.
 - d. All personal data will soon be controlled only by users.
3. Which statement about interoperability is most accurate?
 - a. It means one system owns every other system.
 - b. It occurs automatically whenever a project uses a blockchain.
 - c. It depends on compatible rules, standards, and implementations that allow systems to work together.
 - d. It removes every security risk from connected systems.

TRUE OR FALSE

- » A service that uses a blockchain must be decentralized in every part of its design and operation.

SHORT EXPLANATION

- » In two or three sentences, explain why the statement “Web3 gives every user complete control” should be investigated rather than accepted as a fact.



SUMMARY AND PRACTICAL TAKEAWAYS

- » Web3 is an umbrella term for developing technologies and goals, not one official product or completed upgrade.
- » Common components include blockchain networks, digital assets, smart contracts, decentralized applications, and wallets.
- » Some capabilities already exist, while the broader vision of user control remains an aspiration under development.
- » Digital ownership depends on the system's rules and does not automatically include copyright, physical ownership, universal access, or guaranteed value.
- » Peer-to-peer and permissionless systems still have protocols, conditions, costs, responsibilities, and legal boundaries.
- » Interoperability requires compatible standards and working implementations; a label alone does not create it.
- » A Web3 service may still rely on centralized websites, developers, infrastructure, data providers, or governance.
- » Web3 does not replace every useful Web2 service. The appropriate design depends on the problem and the tradeoffs.
- » Careful learners separate facts and testable capabilities from opinions, forecasts, aspirations, and promotional claims.

The practical goal is to evaluate before accepting. Ask what works now, what remains a goal, who controls each layer, what evidence supports the claim, and what responsibility the participant would carry.

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 Web3 in your own words without using promotional language.
- » Identify two Web3 ideas that appear potentially useful and explain why.
- » Choose one common Web3 claim and classify it as a fact, opinion, forecast, aspiration, or promotional statement.
- » Describe the evidence or questions you would use to evaluate that claim.
- » Explain one reason a Web2 or centralized service may still be appropriate for a particular purpose.

- » End by identifying one question about convenience, control, or responsibility that you want Lesson 4 to help you answer.

Your response should show curiosity and judgment rather than enthusiasm or rejection based only on a label. You do not need to disclose private account, financial, legal, medical, family, or facility information. You are not being asked to create an account, use a wallet, purchase anything, or support one model of the internet over another.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 3: What Is Web3?, 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 3 — [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 in your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, or other sensitive credentials.



UNDERSTANDING WEB3

LESSON 4: CENTRALIZATION, DECENTRALIZATION, AND TRADEOFFS

A Prison Professors Self-Directed Course

Estimated time: 75–110 minutes

Educational Boundary:

This course provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, platform, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this lesson.

OPENING GUIDANCE

In Lesson 3, I encouraged participants to investigate claims before accepting them. The same discipline applies to the words centralized and decentralized. People sometimes use those words as praise or criticism. A person may describe decentralization as automatically fair and centralization as automatically controlling. Another person may describe centralization as automatically efficient and decentralization as automatically disorganized.

Neither label answers the important questions by itself.

I encourage participants to focus on design and responsibility. Ask who keeps the official record, who can change the rules, who corrects an error, what happens when part of the system fails, and what duties fall on the participant. A system may perform well on one measure and poorly on another.

This lesson does not ask you to choose a side. It asks you to compare alternatives. That habit will strengthen critical thinking far beyond Web3. Whenever we make a decision, we should understand what we gain, what we give up, and who carries the consequences.

PURPOSE AND ESSENTIAL QUESTION

Lesson 4 helps participants compare different ways of organizing authority, data, decisions, and responsibility. It explains that centralization and decentralization exist along a range, that many systems combine both approaches, and that every design involves tradeoffs.

Essential Question:

- » How should a careful person compare convenience, control, efficiency, accountability, resilience, and responsibility when evaluating a centralized, decentralized, or mixed system?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define centralization and decentralization.
- » Compare control, efficiency, accountability, resilience, and participant responsibility across different designs.
- » Explain why a distributed system is not necessarily decentralized and why many systems combine centralized and decentralized elements.
- » Explain why decentralization does not automatically produce a fair, safe, or useful result.

KEY TERMS

CENTRALIZATION

Definition: An arrangement in which primary authority, decision-making, or control over a system is concentrated in one organization, person, or governing center.

Sample sentence: The record system uses centralization because one organization maintains the official database and decides who may change it.

DECENTRALIZATION

Definition: An arrangement in which authority, operation, or control is divided among multiple participants or centers rather than concentrated in one governing center.

Sample sentence: The network uses decentralization by allowing independent participants to verify updates under shared rules.

DISTRIBUTED SYSTEM

Definition: A system in which multiple connected computers or locations coordinate to perform work or maintain information.

Sample sentence: A company's service can be a distributed system even when the company controls every computer and policy.



INTERMEDIARY

Definition: A person, organization, or system that stands between other parties and helps coordinate, verify, process, or settle an activity.

Sample sentence: The payment processor acts as an intermediary between a customer and a merchant.

GOVERNANCE

Definition: The rules and processes used to make decisions, assign authority, resolve disputes, and change a system.

Sample sentence: The cooperative's governance rules explain who may vote and how members replace a recordkeeper.

TRADEOFF

Definition: A choice in which gaining an advantage in one area requires accepting a cost, limitation, or increased responsibility in another.

Sample sentence: Faster correction by one administrator may involve a tradeoff because participants must trust that administrator's decisions.

MAIN LESSON

TREAT THE TERMS AS DESCRIPTIONS, NOT SCORECARDS

Centralization and decentralization describe how a system organizes power and work. They do not provide a final grade.

In a centralized arrangement, one organization or governing center has primary authority. It may maintain the official record, approve participants, establish policies, correct mistakes, and decide how the service changes. A bank account system, school enrollment database, or company platform commonly follows this pattern, although each example has different laws and safeguards.

In a decentralized arrangement, authority or operation is divided among multiple participants or centers. They may keep copies of a record, verify updates, vote on changes, or follow a protocol that limits what any one participant can do. A public blockchain is one example. A federation of independent organizations or a cooperative with elected decision-makers can also decentralize some authority without using a blockchain.

These are not two sealed categories. A system can be more centralized in one part and more decentralized in another. The useful question is not simply, "Which label applies?" Ask, "Which function is controlled by whom?"

CENTRALIZED SYSTEMS CAN PROVIDE VALUABLE COORDINATION

Centralized systems often make responsibility easy to locate. If one organization operates the service, participants know who establishes procedures, maintains the technology, answers questions, and corrects an authorized error. The operator can update software, apply a consistent policy, and make urgent decisions without waiting for many independent participants to agree.

This coordination can improve efficiency. A central database can process activity quickly because one authority defines the official version of the record. The organization may offer customer service, password recovery, fraud monitoring, insurance or reimbursement under stated conditions, and a clear complaint process. Laws, contracts, audits, and regulators may create additional accountability, depending on the service and jurisdiction.

Centralization also concentrates power and dependence. The operator may collect sensitive information, change access rules, raise fees, make an incorrect decision, suffer a security failure, or stop providing the service. If the only official record exists under one authority, participants must rely on that authority's competence, integrity, and continued operation.

Concentration can create a single point of failure. That phrase does not always mean one physical computer. A company may operate many computers in several locations and still have one governing authority. If the organization's credentials, decision process, or core service fails, the many machines may not protect participants from the failure.

DECENTRALIZED SYSTEMS DIVIDE AUTHORITY AND RESPONSIBILITY

Decentralization seeks to reduce reliance on one controlling center. Independent participants may verify information according to shared rules. Copies of a record may exist across multiple nodes. A protocol may prevent one operator from changing the record alone.

This design can improve resilience in some circumstances. If one node stops working, others may continue. If no single organization holds exclusive control, one organization's failure or policy decision may have less power over the entire system. Public rules may also allow participants to examine how the system is expected to operate.

Those benefits require coordination. Independent participants need a method for agreeing on valid updates, handling conflicting information, changing rules, and responding to harmful behavior. That process can add cost, delay, technical complexity, or dis-

agreement. It can also make responsibility harder to locate. If something goes wrong, a participant may not find a customer-service office with authority to reverse the result.

Decentralization can transfer duties to users. A person who directly controls an asset may need to protect keys, verify addresses, understand fees, review transactions, and plan for recovery. A network that continues operating despite one user's loss may be resilient at the system level while the loss remains devastating to that individual.

DISTRIBUTED DOES NOT ALWAYS MEAN DECENTRALIZED

A distributed system uses multiple connected computers or locations. Distribution concerns where the work happens. Decentralization concerns how authority and control are divided.

A large company may operate computers in many data centers. The system is distributed because many machines perform the work. It may remain centralized because the company owns the systems, controls the accounts, sets the policies, and decides which software runs.

A decentralized network is usually distributed, but the reverse is not guaranteed. This distinction prevents a common mistake: counting computers without examining who controls them. Ten thousand machines operated under one authority do not create the same governance structure as independent machines operated by unrelated participants.

The same caution applies to blockchain projects. A ledger may be copied across many nodes while a small group controls software development, access to important interfaces, voting power, or information that the blockchain receives from outside sources. A claim of decentralization should identify the layer and the decision being discussed.

INTERMEDIARIES DO MORE THAN STAND IN THE WAY

An intermediary stands between parties and helps coordinate an activity. Banks, marketplaces, payment processors, title companies, schools, courts, and record-keeping organizations can serve as intermediaries in different settings.

Intermediaries may verify identity, preserve records, reduce fraud, enforce agreements, correct mistakes, provide expertise, combine transactions, manage privacy, and resolve disputes. They can also charge fees, create delays, restrict participation, make errors, or misuse power.

A decentralized design may reduce the need for one kind of intermediary, but the work does not disappear. Software developers, network validators, wallet providers, interface operators, data services, auditors, and governance participants may take on parts of the earlier role. Removing one middle layer can create several new relationships.

For that reason, “removes the middleman” is incomplete. A careful learner asks which intermediary is removed, which responsibilities remain, who performs them now, and what protection is lost or gained.

GOVERNANCE EXISTS IN EVERY SYSTEM

Governance is the process for making and changing decisions. A company may use executives, written policies, contracts, and internal controls. A public agency may operate under statutes, regulations, public procedures, and oversight. A cooperative may use member votes. A blockchain community may use technical proposals, developer decisions, validator choices, token voting, or informal agreement.

Rules written in software do not eliminate governance. People decide what code to write, which version to run, how to repair a vulnerability, and whether to accept a change. Even when no person can edit an earlier transaction, people still influence the future rules and the services built around the record.

Good governance makes authority and procedures understandable. Participants should be able to ask: Who proposes a change? Who decides? Who can object? How are conflicts resolved? What happens in an emergency? Who is accountable for a harmful or careless decision?

A decentralized label can hide concentration if only a few participants have the time, technical knowledge, money, or voting power needed to influence decisions. Formal openness does not guarantee equal practical influence.

COMPARE FIVE DIMENSIONS

A disciplined comparison considers several dimensions rather than one slogan.

Control: Who can approve access, change rules, update the official record, or stop an activity? Central control can provide clear authority. Shared control can limit unilateral action. Either can be misused.

Efficiency: How quickly and affordably can the system process work, correct problems, and change? One decision-maker may act quickly. A shared process may require coordination but reduce the need to reconcile separate private records.

Accountability: Who must explain a decision or repair harm? A central operator may provide a clear contact and legal entity. A decentralized network may provide transparent rules but leave no single participant responsible for every outcome.

Resilience: Can the system continue when a machine, organization, or participant fails? Multiple independent operators may reduce dependence on one point. Complexity and shared software can also create failures that affect many participants.

Participant responsibility: What must the user protect, understand, verify, or recover? Convenience often depends on trusting another party. Direct control often requires the participant to carry more security and decision-making duties.

No design maximizes every dimension. Improving one may weaken another. That is the meaning of a tradeoff.

MIXED SYSTEMS ARE COMMON

Many useful systems combine centralized and decentralized elements. A public blockchain may maintain a shared record while a company provides the website. A consortium may share a ledger while approved organizations control membership. A centralized service may use distributed computers and open technical standards. A cooperative may decentralize voting while hiring one team to manage daily operations.

Hybrid design is not automatically a flaw. It may be a deliberate effort to combine shared verification with privacy, customer support, legal accountability, or efficient operations. The danger comes when an organization advertises decentralization without clearly disclosing where control remains concentrated.

DECENTRALIZATION DOES NOT GUARANTEE FAIRNESS OR SAFETY

A decentralized system can still produce unfair outcomes. Early participants may hold more resources or influence. Technical barriers may exclude people without suitable devices, reliable internet, money for fees, or specialized knowledge. Voting can be dominated by a small group. Harmful code can operate consistently. Public records can expose information that should remain private.

Safety also depends on design, testing, governance, education, and human behavior. Distributing a system may reduce one risk while creating another. NIST's Web3 security analysis notes that shifting control toward users can reduce the effect of one large data breach at the system level while making a successful attack on one user especially damaging to that person.

Fairness and safety are outcomes to investigate. They do not come automatically from architecture. Ask who benefits, who carries the burden, who remains excluded, and what remedy exists when harm occurs.

APPLIED SCENARIO: A REENTRY PROGRAM CHOOSES A RECORD SYSTEM

A regional reentry program works with several training providers. It needs an accurate record showing which courses a participant completed. The information may



affect access to services and employment opportunities, so privacy and correction procedures matter.

The program considers three designs.

Centralized database: One nonprofit maintains the official record. Staff at partner organizations submit updates, and the nonprofit verifies them. Participants contact one office to request a correction. This design provides clear accountability and may be efficient, but every partner and participant depends on the nonprofit's security, policies, and continued operation.

Shared consortium record: Each approved training provider maintains a synchronized copy. A written governance agreement identifies who may add records, how organizations resolve conflicts, and how a participant requests a correction. This design divides control among trusted organizations, but coordination and consistent privacy practices require ongoing work.

Public blockchain record: Completion entries are submitted to a public network under its protocol. The network can make later alteration difficult and reduce reliance on one recordkeeper. However, publishing personal information on a public and persistent record could create serious privacy problems. Key management, fees, correction methods, and responsibility for inaccurate entries also require answers.

Reasoned conclusion: The program should not choose a design because one label sounds modern. It should begin with the purpose and the sensitivity of the information. A centralized or consortium design may provide the privacy, correction process, and accountable contact this use requires. If the program uses blockchain technology, it should avoid placing sensitive personal information directly on a public ledger and explain which organization remains responsible for the credential.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF CENTRALIZED DESIGNS

- » One authority can make decisions, maintain consistent procedures, and respond quickly.
- » Participants may have a clear contact for assistance, correction, recovery, or complaints.
- » Privacy and access controls may be easier to manage for sensitive records.
- » A known organization may carry contractual, legal, or regulatory duties.

POSSIBLE BENEFITS OF DECENTRALIZED DESIGNS

- » Multiple independent participants can reduce dependence on one controlling organization.
- » Shared verification can help parties coordinate around one record.
- » Replication may allow a system to continue when one participant or machine fails.
- » Open participation or transparent rules may allow broader inspection and innovation.

IMPORTANT LIMITATIONS AND RISKS

- » Centralized power can be abused, compromised, withdrawn, or applied without sufficient transparency.
- » Decentralized decision-making can be slow, complex, costly, or dominated by a small active group.
- » Public or persistent records can conflict with privacy and correction needs.
- » Greater user control can create greater security and recovery responsibility.
- » A hybrid system can hide important centralized dependencies behind decentralized language.
- » No architecture removes the need for trustworthy software, governance, and human judgment.

COMMON MISCONCEPTIONS

- » “Centralized means one computer.” A centrally governed service may use many distributed machines.
- » “Distributed means decentralized.” Distribution describes the location of work; decentralization describes the division of authority.
- » “An intermediary adds no value.” Intermediaries may verify, coordinate, protect, correct, and resolve disputes, although they can also create costs and risks.
- » “Code eliminates governance.” People still design, adopt, update, and interpret the rules.
- » “Decentralized means no one has power.” Influence may remain concentrated among developers, operators, large holders, or highly active participants.
- » “Decentralization guarantees fairness and safety.” Outcomes depend on access, incentives, governance, implementation, and available remedies.
- » “A system must choose one model.” Many systems use a deliberate combination of centralized and decentralized elements.



ETHICAL PARTICIPATION

Describe control accurately. Do not call an entire service decentralized merely because one component uses a blockchain. Disclose who can change the rules, who controls interfaces or data, and what responsibilities participants must carry.

Protect people before promoting a design. Sensitive personal information should not be placed on a public or difficult-to-correct record without a lawful purpose, appropriate safeguards, and informed consideration of the consequences. Never share or request private keys, seed phrases, passwords, or authentication codes.

OFFLINE EXERCISE: COMPARE THREE RECORD SYSTEMS

Estimated time: 25–30 minutes

Materials: Separate paper and a pen or pencil.

Draw a decision table with these seven column headings:

1. System
2. Who controls the official record?
3. How are updates verified?
4. How are mistakes corrected?
5. Convenience and efficiency
6. Resilience and dependence
7. Participant responsibility and privacy

Create one row for each system below:

Bank ledger: One regulated bank maintains the official account record. Customers use the bank's procedures to authorize transactions, report an error, recover account access, or make a complaint. The bank may use many computers, but it controls the service and official record.

Shared community record: Five community organizations keep matching copies of a resource ledger. Three of the five must approve an update. A written agreement explains membership, corrections, privacy, and disputes. The system does not use a public blockchain.

Public blockchain: Independent network participants validate transactions under a public protocol. The record is replicated across many nodes, and confirmed entries are difficult to alter. Users must protect their authorization credentials and check transaction details. Information recorded publicly may be visible for a long time.



For every cell, write one or two concise sentences. Then answer these questions beneath the table:

- » Which system offers the clearest point of accountability?
- » Which system reduces dependence on one organization?
- » Which system places the greatest direct responsibility on the participant?
- » Which system may make an authorized correction easiest? Which may make it hardest?
- » Which design would you choose for a private medical record, a public donation ledger, or a small organization's supply inventory? Explain why the answer may differ by purpose.

There is no single best row. Support each conclusion with the facts in the scenario and identify at least one tradeoff.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best explains the difference between a distributed system and a decentralized system?
 - a. A distributed system always has no governing authority.
 - b. Distribution describes where computers perform work; decentralization describes how authority and control are divided.
 - c. A decentralized system must operate from one computer.
 - d. The terms have exactly the same meaning.
2. Which statement best describes an intermediary?
 - a. An organization or system that may coordinate, verify, process, or settle activity between parties
 - b. A computer that cannot communicate with another computer
 - c. A person who automatically controls every decentralized network
 - d. A rule that eliminates the need for governance
3. Which conclusion demonstrates tradeoff thinking?
 - a. Centralized systems are always efficient and safe.
 - b. Decentralized systems are always fair and resilient.
 - c. A central operator may provide convenient recovery, while direct user control may reduce dependence but increase security responsibility.

- d. The system with the greatest number of computers is always the best choice.

TRUE OR FALSE

- » Decentralizing one component of a service guarantees that the entire service is decentralized, fair, and safe.

SHORT EXPLANATION

- » In two or three sentences, explain how convenience and control can create a tradeoff when a person chooses between an account managed by an organization and a system the person controls more directly.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Centralization concentrates primary authority in one organization, person, or governing center.
- » Decentralization divides authority, operation, or control among multiple participants or centers.
- » A distributed system uses multiple computers or locations but may remain centrally governed.
- » Centralized designs can offer efficiency, consistent procedures, support, recovery, and clear accountability.
- » Decentralized designs can reduce dependence on one operator, support shared verification, and improve some forms of resilience.
- » Intermediaries may create value as well as cost. Removing one intermediary transfers its work and risk to other participants or systems.
- » Governance exists in centralized, decentralized, and hybrid systems.
- » Control, efficiency, accountability, resilience, and participant responsibility should be compared together.
- » Many useful systems combine centralized and decentralized elements.
- » Decentralization does not automatically produce fairness, safety, privacy, or equal influence.

The practical goal is to identify the tradeoff before making a judgment. Ask which design fits the purpose, who controls each layer, who carries responsibility, and what remedy exists when something goes wrong.

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 centralization and decentralization in your own words.
- » Identify one centralized service that offers useful convenience or accountability and explain the tradeoff involving control or dependence.
- » Describe one activity that could benefit from shared or decentralized control and explain why.
- » Compare who would carry responsibility in the two examples.
- » Explain why decentralization should not be treated as a guarantee of fairness or safety.
- » End with two questions you would ask before choosing a centralized, decentralized, or mixed design.

Your response should demonstrate comparison rather than loyalty to a label. You do not need to disclose private account, financial, legal, medical, family, or facility information. You are not being asked to open an account, use a wallet, purchase anything, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 4: Centralization, Decentralization, and Tradeoffs, 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 4 — [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 in your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, or other sensitive credentials.

UNDERSTANDING WEB3

SECTION 1 REVIEW: UNDERSTANDING THE INTERNET AND WEB3

A Prison Professors Self-Directed Course

Estimated time: 60–90 minutes

Educational Boundary:

This review provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this review.

REVIEW PURPOSE

You have completed the first four lessons of Understanding Web3. This review gives you a place to pause, strengthen your vocabulary, and apply the ideas before moving into blockchain foundations.

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, study the relevant passage, and revise your response. That cycle can help you develop the habits of a self-directed learner.

THE REVIEW COVERS:

- » Becoming your own prison professor through self-directed learning and critical thinking.
- » The relationship between the internet, the early web, and Web2.
- » A careful definition of Web3 and the difference between a capability and a promotional claim.
- » Centralization, decentralization, distributed systems, governance, and tradeoffs.

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 compare alternatives.
- » 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, 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 complete.

PART 1: KNOWLEDGE QUESTIONS

MULTIPLE CHOICE

1. Which action best demonstrates self-directed learning?
 - a. Waiting for perfect conditions before beginning
 - b. Setting a goal, using available resources, checking understanding, and adjusting the plan
 - c. Repeating a technical definition without examining it
 - d. Assuming that finishing a page proves mastery
2. Which statement accurately describes a boundary of this course?
 - a. It provides general technology education rather than individualized financial, legal, or tax advice.
 - b. It recommends a digital asset for each participant.
 - c. It requires every participant to create an online account.
 - d. It guarantees a job or financial opportunity after completion.
3. Which statement best describes the relationship between the internet and the World Wide Web?
 - a. They are two names for exactly the same system.
 - b. The web is one major service that operates through the broader internet.
 - c. The internet was created after Web2.
 - d. The web includes only social-media platforms.
4. Which activity most clearly reflects a Web2 pattern?
 - a. Reading a fixed page that only its publisher can update
 - b. Creating an account, uploading a video, and responding to comments
 - c. Writing a paper journal entry without using a device



- d. Following a printed table of contents
- 5. Which statement accurately describes a centralized online service?
 - a. It must operate from one physical computer.
 - b. It cannot include user-generated content.
 - c. One organization has primary authority over its accounts, rules, and systems.
 - d. Every user has equal power to change its policies.
- 6. Which statement best defines Web3 for this course?
 - a. One finished product that replaced Web2 on a specific date
 - b. Any website that accepts an online payment
 - c. A broad set of developing technologies and ideas involving block-chains, digital assets, programmable rules, and decentralized designs
 - d. A guarantee that every participant controls every part of an online service
- 7. Which statement describes an established technical capability rather than an aspiration, forecast, or promotion?
 - a. Web3 will make every online service fair.
 - b. This public blockchain records token transfers according to its protocol.
 - c. This token is guaranteed to change your life.
 - d. Every employer will soon accept the same digital credential.

TRUE OR FALSE

- 1. Web2 began on one official date when every website received the same technical upgrade.
- 2. A system can distribute work across many computers while one organization still controls its rules, accounts, and important decisions.

SHORT EXPLANATION

- » In three to five sentences, explain why decentralization does not automatically make a system fair, safe, or useful. Identify one question a careful learner should ask before deciding whether a centralized or decentralized design fits a particular purpose.

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. Self-directed learning
- b. Critical thinking
- c. Internet
- d. Early web
- e. Web2
- f. Platform
- g. Web3
- h. Protocol
- i. Permissionless
- j. Centralization
- k. Decentralization
- l. Tradeoff

DEFINITIONS

1. A choice in which gaining an advantage in one area requires accepting a cost, limitation, or increased responsibility in another.
2. A digital service that organizes interactions among different groups of users.
3. A broad label for a more participatory web in which people commonly create accounts, contribute content, interact with others, and use online services.
4. An arrangement in which primary authority, decision-making, or control is concentrated in one governing center.
5. A worldwide system of connected computer networks that exchange information by following shared technical rules.
6. A learning process in which a person takes active responsibility for goals, resources, progress, and understanding.
7. A set of technical rules that allows computers or network participants to communicate and coordinate.
8. A broad label for the first period of the World Wide Web, when many sites primarily published linked pages for visitors to read.
9. An arrangement in which authority, operation, or control is divided among multiple participants or centers.
10. The disciplined practice of asking questions, examining evidence, recognizing assumptions, and reaching a reasoned conclusion.

11. Open to participation under a system's rules without advance approval from a central administrator.
12. A broad and still-developing term for technologies and ideas that use decentralized networks, blockchains, digital assets, and programmable rules to create new ways to interact.

PART 3: APPLIED SCENARIO — A SHARED COMMUNITY RESOURCE RECORD

Four community organizations help people find lawful employment training, transportation, food assistance, and educational programs. The organizations want one digital record that lists available services, eligibility requirements, contact information, and the date each listing was last verified. The record will not contain participants' private information.

The organizations are comparing two designs.

Design A — One organization maintains the record: One nonprofit operates the official database. Staff members from the other organizations send updates to that nonprofit. The nonprofit checks the information, publishes changes, corrects errors, and answers questions. This design creates one accountable contact and may allow fast, consistent decisions. The other organizations must depend on the nonprofit's security, staffing, policies, and continued operation.

Design B — The organizations maintain a shared record: Each of the four organizations keeps a synchronized copy. Shared technical rules explain how an approved organization proposes an update. At least two organizations must verify an important change before it becomes part of the record. A governance agreement explains how the group resolves disagreements and replaces an organization that stops participating. This design divides control and reduces reliance on one recordkeeper. It also requires coordination, compatible systems, clear responsibilities, and a process for correcting inaccurate information.

SCENARIO QUESTIONS

1. Which design concentrates decision-making authority, and which design divides authority among several participants? Explain your answer.
2. Compare accountability in the two designs. If a listing is wrong, who should be responsible for investigating and correcting it?
3. Which design may allow a routine correction to be made more quickly? What tradeoff may come with that advantage?



4. Which design may remain available if one organization has a technical failure or closes? What facts would you need before reaching a firm conclusion?
5. Identify two governance rules that Design B would need in addition to the rules already described.
6. Recommend Design A, Design B, or a carefully explained combination for this purpose. Support your recommendation with at least two reasons, and identify one limitation or responsibility that the organizations would still need to manage.

COMPLETION CHECK

Before moving to Section 2, ask yourself whether you can:

- » Explain how self-directed learning and critical thinking strengthen preparation.
- » Distinguish the internet, the early web, Web2, and Web3 without treating the labels as exact dates or complete replacements.
- » Separate an established capability from an aspiration, forecast, opinion, or promotional claim.
- » Compare centralized and decentralized designs by examining purpose, control, efficiency, accountability, resilience, governance, and participant responsibility.
- » Identify a tradeoff without assuming that one design is always better.

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

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 1 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 1 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, or other sensitive credentials.

UNDERSTANDING WEB3

LESSON 5: WHAT IS A BLOCKCHAIN?

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson explains technology. It does not recommend any network, company, product, or digital asset. It does not provide financial, investment, legal, or tax advice. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.

OPENING GUIDANCE

While serving 26 years in federal prison, I learned that self-directed study begins with reading, developing a vocabulary, and practicing how to communicate. Blockchain may sound highly technical, but you can build an accurate understanding one idea at a time. Your goal is not to repeat somebody else's definition. Your goal is to explain the concept clearly, question its limitations, and create a written record of what you are learning. That process is part of becoming your own prison professor.

PURPOSE AND ESSENTIAL QUESTION

A blockchain is one of the central technologies behind Web3. Later lessons will examine blocks, transactions, hashes, networks, digital assets, wallets, and smart contracts. Before studying those details, you need a reliable mental model of the whole system.

Essential Question:

- » How can a group maintain a shared digital record, and what can a blockchain do—or fail to do—for that group?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define a blockchain as a type of shared digital ledger.
- » Explain why records are grouped into blocks and linked in sequence.
- » Describe how multiple participants maintain and verify a record.
- » Identify situations in which a blockchain may or may not be useful.
- » Explain one important limitation or misconception in your own words.

KEY TERMS

BLOCKCHAIN

Definition: A shared digital ledger in which records are grouped into blocks, linked in order, and maintained according to a network's rules.

Sample sentence: The organizations considered using a blockchain so they could compare the same shared record.

LEDGER

Definition: An organized record of transactions, events, balances, or other changes.

Sample sentence: The supply clerk updated the ledger after issuing five notebooks.

RECORD

Definition: Stored information about an event, item, person, or change.

Sample sentence: Each course completion created a new record in the credential system.

TRANSACTION

Definition: A proposed action or change that a system may verify and add to its record. A transaction does not have to involve money.

Sample sentence: Updating the registered owner of a digital item is one type of transaction.

BLOCK

Definition: A group of accepted records or transactions stored together in a blockchain.

Sample sentence: The network added the verified transactions to the next block.

NETWORK

Definition: A group of connected computers or participants that exchange information and follow shared rules.

Sample sentence: Computers in the network compared information before accepting the update.

MAIN LESSON

BEGIN WITH THE IDEA OF A LEDGER

People have used ledgers for centuries. A store may keep a ledger of sales. A school may maintain a record of completed courses. A warehouse may track items received and issued. The form may be a bound book, a spreadsheet, or a database. In every case, the purpose is similar: preserve an organized history that people can consult.

A ledger becomes difficult to manage when several people or organizations need to rely on it but do not want one party to have complete control. Imagine that three organizations jointly operate a training program. One delivers instruction, one verifies completion, and one helps employers evaluate credentials. They all need accurate information. If only one organization controls the database, the others must trust that organization to enter records correctly, protect the system, and remain available.

A blockchain offers another way to organize the record. Instead of relying only on one central copy, participants in a network can maintain copies or independently verify the shared history. The network uses agreed rules to decide which proposed updates are accepted. Accepted records are grouped into blocks, and each new block is connected to the earlier history.

This does not eliminate trust. It changes where trust is placed. Participants may rely less on one recordkeeper and more on software, network rules, validators, governance, and the behavior of multiple participants. Those parts can also fail or be misused. Responsible analysis asks not whether a system is “trustless,” but what must be trusted and what evidence supports that trust.

WHY USE BLOCKS?

A busy system may receive many proposed transactions. Handling them one at a time across a network could make coordination difficult. A blockchain groups accepted transactions into batches called blocks. The block provides an ordered package that participants can verify and add to their copies of the ledger.

Think of a block as one numbered page in a permanent logbook. Several entries appear on the page. When the page is complete and accepted, the next page begins. This analogy helps explain grouping and order, but it has limits. A real blockchain uses digital data, cryptographic methods, and network rules—not paper, ink, or a physical binding.

Figure 1. Simplified blockchain structure

Each block contains records and a reference to the previous block. The arrows are implied by the references. This diagram simplifies a real network.

The diagram shows the basic sequence. Records are grouped into a block. The next block includes its own records and a cryptographic reference to the earlier block. Later lessons will explain hashes, which help create those references. For now, the important point is that the blocks form an ordered history rather than a collection of unrelated files.

WHY LINK THE BLOCKS?

The link between blocks helps make changes detectable. If someone alters information in an earlier block, the cryptographic reference associated with that block changes. Later links no longer match the altered history. Network participants can detect the disagreement by comparing the data and applying the network's rules.

For this reason, careful sources describe blockchains as tamper-evident and tamper-resistant. Those terms are more accurate than saying a blockchain is “impossible to change.” Different systems have different designs. A network may correct an error through a later transaction. Participants may also adopt new software rules, reorganize recent history under limited conditions, or create a separate version of a network. The strength of the record depends on the technology, number and independence of participants, incentives, governance, and security practices.

Linking also helps preserve order. If Block 12 points back to Block 11, and Block 11 points back to Block 10, participants can follow the sequence of accepted events. Order matters when two proposed actions conflict—for example, when a system must determine which change happened first.

HOW PARTICIPANTS MAINTAIN A SHARED RECORD

A blockchain operates through a network. Computers in that network are often called nodes. Depending on the system, some nodes store the history, some check proposed transactions, and some help produce or approve new blocks. The exact roles differ across networks.

The network needs common rules. Those rules may address questions such as:

- » What makes a proposed transaction valid?
- » Who may propose or approve a block?
- » How do participants respond if they receive conflicting versions?
- » What happens when a participant is offline or behaves dishonestly?
- » How can the rules change in the future?

The process by which a network reaches agreement is generally called consensus. Consensus will receive fuller treatment in a later lesson. At this stage, remember

that a blockchain is not merely a chain-shaped file. It is a record plus a network of participants, technical controls, and rules for accepting updates.

Copies of the ledger may not be perfectly synchronized at every instant. Information takes time to move across a network. Still, the system aims to bring participants to an accepted history under its rules. That shared history can allow parties to coordinate even when they are located in different places or do not want one party to be the only recordkeeper.

A BRIEF APPLIED EXAMPLE: BNB SMART CHAIN

BNB Smart Chain is one example of a public blockchain network. Its official documentation describes validators that take turns producing blocks under rules connected to staking and governance. Other network participants can receive and check the resulting blockchain data.

This example illustrates an important point: “shared” does not mean that every person creates every block. Networks assign different roles and make different design choices. BNB Smart Chain uses a limited validator set, while Bitcoin, Ethereum, and other networks use different methods. Each approach involves tradeoffs involving participation, performance, security, cost, and concentration of influence. Mentioning BNB Smart Chain here is an educational example, not an endorsement or an invitation to acquire BNB.

WHEN MIGHT A BLOCKCHAIN BE USEFUL?

A blockchain may deserve consideration when several participants need a shared record, no single participant should control the only copy, and the group needs a dependable way to detect changes and agree on updates. Possible areas include tracking items across organizations, recording digital credentials, coordinating a registry, or documenting transfers of digital assets.

Return to the training-program example. A shared credential registry could help authorized participants determine whether a record was issued and whether it was later changed. A learner might be able to present evidence of completion without depending on one office being open. Those are possible benefits, not guaranteed results.

Before choosing a blockchain, the program should ask difficult questions. Who may view the records? Who corrects an error? Should personal information be stored in a system designed to preserve history? What happens if the software is unavailable? Who pays the operating cost? Who controls rule changes? Would a conventional database managed by a trusted organization be simpler, faster, less expensive, and more private?

If one reliable organization already has clear authority to maintain the record, a normal database may be the better choice. Blockchain adds coordination, technical, and governance costs. Using it only because the word sounds modern is not responsible innovation.

WHAT A BLOCKCHAIN DOES NOT GUARANTEE

A blockchain can help protect the integrity of recorded data, but it cannot guarantee that the original information was true. If a person enters a false course-completion record and the system accepts it, the blockchain may preserve that false statement very effectively. People sometimes summarize this problem as “garbage in, garbage out.” Verification before entry still matters.

A blockchain also does not guarantee privacy, fairness, safety, or equal power. A public record may expose information that should not be permanent. People with more technical knowledge, money, voting power, or control over infrastructure may have greater influence. Software may contain errors. Users may be deceived. Governance decisions may favor some participants over others.

The ethical question is not simply, “Can we put this information on a blockchain?” It is also, “Should we?” A responsible design protects privacy, limits unnecessary data, provides a fair correction process, explains who has power, and considers people who cannot easily use the technology.

APPLIED SCENARIO: A SHARED CREDENTIAL RECORD

Three organizations want to record completion of a job-readiness program. They are considering a blockchain because each organization wants to verify the same history. The proposal could reduce dependence on one database administrator and make later changes easier to detect.

However, the record may contain personal information. A mistake could be difficult to correct. The organizations have not decided who may approve records, how participants can challenge an error, or whether employers should see every detail. A conventional database with access controls might meet the need with less complexity.

Reasoned conclusion: Blockchain is one possible tool, but the organizations do not yet have enough information to select it responsibly. They should first define the problem, privacy requirements, governance rules, correction process, costs, and alternatives.



BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Several participants can verify a shared history.
- » Linked blocks can make later alteration easier to detect.
- » Multiple copies may reduce dependence on one central database.
- » Agreed rules can help organizations coordinate updates.

IMPORTANT LIMITATIONS AND RISKS

- » A blockchain may be slower, more complex, or more expensive than an ordinary database.
- » Permanent or widely shared records can create privacy problems.
- » Incorrect information can still be entered and preserved.
- » Software, validators, node operators, and governance processes can fail or be attacked.
- » Influence may be concentrated even when a system is described as decentralized.

COMMON MISCONCEPTIONS

- » “Blockchain and Bitcoin mean the same thing.” Bitcoin uses a blockchain, but blockchain is a broader recordkeeping design used by different networks.
- » “A blockchain makes every record true.” It can help preserve accepted data; it cannot prove that every outside claim was accurate when entered.
- » “No person or institution has power.” People design the software, operate infrastructure, make governance decisions, and control access in many systems.
- » “Blockchain is always better than a database.” The better tool depends on the problem, participants, costs, privacy needs, and available alternatives.
- » “Blockchain records can never change.” Tamper-evident and tamper-resistant are more accurate descriptions than absolutely unchangeable.

OFFLINE EXERCISE: THE THREE-COPY LEDGER

Estimated time: 15–20 minutes

Materials: Three sheets of paper and a pencil. A calculator is not required.

You may complete this exercise alone. If you are working in a group, assign one sheet to each of three recordkeepers.

SET UP THE LEDGERS

1. Label the sheets Ledger A, Ledger B, and Ledger C.
2. Write the starting record on each sheet: Supply-room notebook balance: 20.
3. Copy these proposed transactions onto each sheet:
4. Issue 3 notebooks to Study Group One.
5. Receive 5 new notebooks from the warehouse.
6. Issue 4 notebooks to Study Group Two.

VERIFY AND GROUP THE RECORDS

1. Verify the balance after each transaction. The balances should be 17, then 22, then 18.
2. Group Transactions 1 and 2 into Block 1. Group Transaction 3 into Block 2.
3. On Block 2, write: Previous block reference: Block 1.

CREATE AND RESOLVE A DISAGREEMENT

1. On Ledger C only, change Transaction 2 from “receive 5” to “receive 6.” Its final balance becomes 19.
2. Compare the three ledgers. Circle the disagreement.
3. Return to the original transaction list, apply the shared rule that every entry must match the authorized list, and correct Ledger C.

REFLECT ON THE SIMULATION

Write brief notes answering these questions:

- » What did comparing several copies reveal?
- » Why did the group need an original source and a shared verification rule?
- » If the original transaction list had contained false information, would three matching copies have made it true?
- » What parts of a real blockchain did this exercise leave out?

Important limitation of the simulation: A real blockchain uses computers, digital signatures, cryptographic links, and formal consensus rules. This paper activity demonstrates shared copies, grouped records, sequence, verification, and disagreement. It does not reproduce the security of a real blockchain.



KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes a blockchain?
 - a. A guaranteed way to make every stored statement true
 - b. A shared digital ledger that groups records into linked blocks
 - c. A private password used to open a financial account
 - d. A name for every ordinary database
2. Why are blocks linked in sequence?
 - a. To help preserve order and make changes to earlier history detectable
 - b. To guarantee that no software bug can exist
 - c. To hide every transaction from network participants
 - d. To eliminate the need for rules and governance
3. Which situation provides the strongest reason to consider a blockchain?
 - a. One trusted office needs a simple private list that only it will use
 - b. A team wants to use a fashionable word in its advertising
 - c. Several organizations need to coordinate a shared record without giving one party sole control
 - d. A person wants a system that will correct all false information automatically

TRUE OR FALSE

- » If several blockchain participants agree on a record, that agreement proves the original information came from an honest and accurate source.

SHORT EXPLANATION

- » In two or three sentences, explain one possible benefit of a blockchain and one limitation that decision-makers should examine before using it.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A blockchain is a type of shared digital ledger.
- » Records or transactions are grouped into blocks and linked in sequence.
- » A network follows rules to verify updates and maintain an accepted history.
- » A blockchain can make changes easier to detect, but it cannot guarantee that the original information was true.



- » Blockchain is not automatically better than a conventional database. A responsible decision compares the problem, benefits, risks, privacy needs, governance, costs, and alternatives.

The most useful skill is not memorizing a slogan. It is being able to explain the system accurately, recognize what it does not guarantee, and ask whether it fits the problem.

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 a blockchain in your own words. Use the ideas of a ledger, blocks, links, and a network.
- » Describe one situation in which a shared record could be useful.
- » Identify at least one limitation, risk, or unanswered question that should be considered.
- » Explain how verifying information and comparing alternatives can strengthen your critical-thinking or decision-making skills.
- » End with one practical takeaway or question that you want to carry into the next lesson.

Your response should demonstrate your reasoning. You are not being asked to support or oppose blockchain technology, purchase anything, create an account, or disclose private financial information.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 5: What Is a Blockchain?, 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 5 — [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, or other sensitive credentials.

PRISON PROFESSORS CHARITABLE CORPORATION

Prison Professors Charitable Corporation / 1205 BMC Drive / Suite #706 / Cedar Park, TX 78613
IRS 501c3 #85-2603315 / www.PrisonProfessors.org



UNDERSTANDING WEB3**LESSON 6: BLOCKS, TRANSACTIONS, AND HASHES**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson explains technology. It does not recommend any network, company, product, or digital asset. It does not provide individualized financial, investment, legal, or tax advice. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.

OPENING GUIDANCE

Lesson 5 introduced a blockchain as a shared digital ledger. In this lesson, we will slow the process down and examine how a proposed transaction can become part of a block and how hashes help connect one block to the next.

When I encounter a technical subject, I find it useful to separate the process into smaller questions. What information is being proposed? Who or what checks it? How is it grouped? What evidence would reveal a later change? I encourage you to use that method here. You do not need to memorize a formula or become a cryptographer. Your goal is to build a mental model that you can explain accurately, test against an example, and improve through writing.

Careful wording is part of the lesson. People often say that blockchain records are “immutable,” meaning they cannot change. That single word may hide important conditions and tradeoffs. By the end of the lesson, you should be able to explain why tamper-evident and tamper-resistant are usually more responsible descriptions.

PURPOSE AND ESSENTIAL QUESTION

Lesson 6 explains how transaction information moves toward an accepted block, what a cryptographic hash does, and why a chain of hash references can make altered records detectable.

Essential Question:

- » How do transactions, blocks, and hashes work together to create an ordered record, and what does that structure prove—or fail to prove?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Describe the basic path from a proposed transaction to a recorded block.
- » Define a cryptographic hash in beginner-friendly language.
- » Explain how linked hashes help make altered records detectable.
- » Distinguish tamper-evident from impossible to change.
- » Identify one thing a hash can show and one thing it cannot prove.

KEY TERMS

TRANSACTION

Definition: A proposed action or change that a system may verify and add to its record. A transaction does not have to involve money.

Sample sentence: Recording that an organization issued a digital credential can be treated as a transaction.

BLOCK

Definition: A group of accepted records or transactions stored together in a blockchain.

Sample sentence: The validator included several accepted transactions in the next block.

HASH

Definition: A fixed-length result produced when a hash function processes data. A cryptographic hash is designed so that a change to the input produces a different result and so that reversing the result or finding two matching inputs is extremely difficult.

Sample sentence: The learner compared the two hashes to see whether the recorded data had changed.

CRYPTOGRAPHY

Definition: The study and use of mathematical methods that help protect information and support functions such as confidentiality, integrity, authentication, and verification.

Sample sentence: A blockchain uses cryptography as one part of its security design, but cryptography does not remove the need for sound rules and responsible participants.

TIMESTAMP

Definition: Time-related information attached to a record or block according to a system's rules.

Sample sentence: The block included a timestamp that helped place it within the network's sequence.

TAMPER-EVIDENT

Definition: Designed so that an unauthorized or unexpected change leaves evidence that can be detected.

Sample sentence: The linked references made the record tamper-evident because changing an earlier block caused later references to stop matching.

MAIN LESSON

BEGIN WITH A PROPOSED TRANSACTION

A transaction begins as a proposed change. In a payment system, it might propose transferring a digital asset. In a credential system, it might propose recording that an authorized organization issued or revoked a credential. In a supply system, it might propose changing the recorded quantity of an item.

The word transaction describes a system event, not necessarily a purchase. The important question is what change the system is being asked to recognize.

A proposed transaction is not automatically an accepted fact. The system first applies its rules. Depending on the network, those rules may check the format, authorization, digital signature, available balance, sequence number, or other conditions. A transaction that fails the applicable checks should not enter an accepted block.

Passing those checks still does not prove that every statement about the outside world is true. If an authorized person submits an incorrect course-completion record, the transaction may be technically valid even though the underlying claim is false. Blockchains can check information that exists within their rules. They cannot independently observe every real-world event.



THE BASIC PATH FROM TRANSACTION TO BLOCK

Different blockchain networks use different procedures, but a beginner can understand the general path in five stages.

1. Proposal: A participant creates and submits a transaction in the form required by the network.
2. Initial checking: Network software checks whether the transaction satisfies basic rules.
3. Selection and grouping: A miner, validator, or other authorized process selects acceptable transactions and groups them into a proposed block.
4. Network agreement: Participants apply the network's consensus rules to decide whether the proposed block becomes part of the accepted history.
5. Recording and distribution: The accepted block is linked to the earlier block and shared across the network's copies of the ledger.

Lesson 7 will examine nodes, validators, miners, and consensus mechanisms more closely. For now, notice that a transaction does not move directly from one person's request into permanent history. A system of checks, roles, and rules stands between the proposal and the accepted block.

There may also be a delay. A transaction can wait before selection. A block can be proposed before the network treats it as final. Some networks may temporarily disagree about the most recent history and later settle on one version under their rules. Words such as pending, included, confirmed, and finalized can describe different stages. They should not be treated as exact synonyms.

WHAT A HASH DOES

A hash function accepts input data and produces an output called a hash, hash value, or message digest. For a particular hash algorithm, the output has a fixed length even when the input varies in length.

Imagine placing a document into a machine that produces a short code. The same document processed by the same machine produces the same code. Change one character in the document, and the code changes. That analogy is useful, but it has limits. A real cryptographic hash function uses mathematics, not a physical machine, and the output may appear as a long string of numbers and letters.

Secure cryptographic hash functions are designed around several properties:

- » Deterministic: The same input processed by the same hash function produces the same output.

- » Fixed-length output: A chosen algorithm produces an output of a set length even when inputs have different lengths.
- » Sensitive to change: A small change in the input should produce a different-looking output.
- » One-way in practice: It should be computationally infeasible to work backward from the hash and recover the original input.
- » Collision-resistant: It should be computationally infeasible to find two different inputs that produce the same hash.

Collision-resistant does not mean that matching outputs are mathematically impossible. A fixed-length output has a limited number of possible values, while possible inputs are far more numerous. Secure algorithms are designed to make a useful collision extraordinarily difficult to find. The strength also depends on using an appropriate algorithm and implementing it correctly.

A HASH IS NOT ENCRYPTION

Hashing and encryption are related to cryptography, but they perform different jobs.

Encryption transforms readable information into a protected form that an authorized person can reverse with the proper key. A cryptographic hash is intended to be one-way. It produces a digest used for comparison or as part of another security process. It is not a container that someone later opens to recover the original message.

A hash also does not automatically hide the input. If someone knows a small set of possible inputs, that person may hash each possibility and compare the results. Sensitive information should not be placed on a public blockchain merely because the system stores or references a hash. Privacy decisions require a broader analysis.

HOW HASHES LINK BLOCKS

In a simplified blockchain model, each block includes transactions, time-related information, and a reference derived from the previous block's data. That reference is commonly a cryptographic hash.

Suppose Block 20 contains a hash of Block 19. Block 21 then contains a hash of Block 20. If someone changes a transaction in Block 19, the hash calculated for Block 19 changes. The reference stored in Block 20 no longer matches the altered Block 19. That mismatch creates evidence that the chain has been changed.

Recalculating one hash would not be enough to hide the alteration. The person would also need to rebuild the later references and overcome the network's rules for accept-



ing history. As more blocks are added and more independent participants maintain the accepted chain, rewriting older history may become increasingly difficult.

The hash link provides tamper evidence. The network, consensus process, participant independence, software security, and incentives help provide tamper resistance. A hash alone does not make a record impossible to change.

WHAT A TIMESTAMP CAN AND CANNOT SHOW

A timestamp helps place a transaction or block in time according to a system's rules. It can support ordering and help participants evaluate whether information fits the expected sequence.

A timestamp should not be treated as perfect proof that an outside event occurred at an exact moment. Networks differ in who supplies time information, how much variation their rules permit, and when a proposed block becomes accepted. The timestamp belongs to the technical record. Additional evidence may be needed to prove when a real-world event happened.

WHY "IMMUTABLE" REQUIRES CAREFUL EXPLANATION

The word immutable literally suggests that something cannot change. In ordinary blockchain discussion, people often use it more loosely to mean that accepted history is difficult to alter without detection.

Several situations show why precision matters:

- » A network may correct an error by adding a later transaction rather than erasing the earlier one.
- » Recent blocks may be reorganized if the network temporarily received competing versions of history.
- » Participants may adopt new software rules or split into separate networks.
- » A private or permissioned system may give administrators defined powers to change or replace records.
- » A poorly secured or highly concentrated network may be more vulnerable to coordinated alteration.

For those reasons, tamper-evident describes the evidence left by a change, while tamper-resistant describes the difficulty of making an accepted change succeed. Neither phrase claims that alteration is impossible under every condition.

A BRIEF APPLIED EXAMPLE: BNB SMART CHAIN

As of July 20, 2026, BNB Chain's official documentation describes BNB Smart Chain as a network in which validators produce blocks under its consensus rules. Its developer documentation also describes methods for retrieving transactions from a block and locating transaction data by a transaction hash.

This provides a practical use of hash language. A transaction hash can act as an identifier that lets software or a block explorer locate the transaction record. A block has its own hash-based references within the chain. These identifiers help people compare records and follow the sequence.

The transaction hash does not prove that every outside statement connected with the transaction was accurate. It also does not, by itself, prove that the transaction succeeded, became final, or was authorized by the right real-world person. A careful reviewer examines the transaction data, its status or receipt, the block, the network, and the surrounding evidence.

Mentioning BNB Smart Chain is an educational example. It is not an endorsement, an invitation to acquire BNB, or a request to conduct a transaction.

WHAT HASHES CANNOT PROVE

Hashes are useful for integrity checks, but their limits matter.

A matching hash can show that the compared data produced the same digest under the same function. It does not prove:

- » That the original information was truthful.
- » That the person who submitted it had lawful authority.
- » That a record was fair, complete, private, or ethically collected.
- » That the software or hash function was implemented correctly.
- » That the broader network is secure or decentralized.
- » That an outside event occurred exactly as described.

Other tools and procedures address those questions. Digital signatures can help check authorization. Governance rules can assign responsibility. Privacy controls can limit access. Audits and source documents can help verify outside facts. No single technical feature replaces the entire system of judgment.

APPLIED SCENARIO: A FOOD-DISTRIBUTION RECORD

Three nonprofit warehouses coordinate deliveries of shelf-stable food. Each warehouse submits daily records showing the number of cases received and distributed.



The organizations use a shared chain of blocks. Each new block contains accepted records and a hash reference to the previous block.

An auditor later receives two copies of the history. In the first copy, Block 8 says that Warehouse B received 80 cases. In the second copy, the entry says 60 cases. The two versions produce different hashes, and the later references match only the first copy.

The hash comparison reveals that one version was changed. It does not prove that 80 cases actually arrived. The original delivery receipt may have been wrong, the data-entry person may have made a mistake, or an authorized person may have submitted false information.

Reasoned conclusion: The linked hashes help the auditor detect a disagreement and identify which history matches the later chain. The organizations still need source documents, authorized submitters, correction procedures, and accountability. Technical integrity and factual truth are related, but they are not the same.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Hashes provide a practical way to compare data and detect change.
- » Linked hashes help preserve an ordered relationship among blocks.
- » Multiple participants can compare the chain and identify a conflicting version.
- » Later blocks can make rewriting older accepted history more difficult.

IMPORTANT LIMITATIONS AND RISKS

- » A hash cannot prove that the original input was true or lawfully authorized.
- » Weak or outdated hash functions may not provide the expected protection.
- » Poor implementation can undermine a strong cryptographic design.
- » Public records or predictable inputs can create privacy risks even when hashes are used.
- » Network concentration, software defects, governance failures, or attacks can weaken tamper resistance.
- » A timestamp may not prove the exact time of an outside event.

COMMON MISCONCEPTIONS

- » “A transaction always means a payment.” A transaction can represent many proposed changes to a system’s record.



- » “A transaction is permanent as soon as it is submitted.” It may be pending, rejected, included, confirmed, reorganized, or finalized depending on the network and stage.
- » “A hash encrypts the original information.” Hashing produces a one-way digest; encryption is designed to be reversed with the proper key.
- » “Different inputs can never share a hash.” Secure functions make useful collisions extremely difficult to find, not mathematically impossible.
- » “A matching hash proves the information is true.” It supports an integrity comparison, not verification of every outside fact.
- » “Immutable means nobody can ever change anything.” Responsible analysis examines the network’s rules and uses more precise terms such as tamper-evident and tamper-resistant.

OFFLINE EXERCISE: BUILD A PAPER HASH CHAIN

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil. A calculator is optional.

This exercise uses a simple two-digit check code to demonstrate linked references. The code is not secure and is not a real cryptographic hash. It is intentionally simple enough to calculate on paper.

USE THE TOY RULE

FOR EACH BLOCK, CALCULATE:

Toy hash = previous hash + block number + quantity + number of words in the transaction. Keep only the final two digits.

Count Receive, Issue, the number, and the item as words. For example, “Receive 5 books” contains three words. Begin with previous hash 00.

BUILD THE CHAIN

» Block 1

Previous hash: 00

Transaction: Receive 5 books

Calculation: $00 + 1 + 5 + 3 = 09$

Toy hash: 09

» Block 2



Previous hash: 09

Transaction: Issue 2 books

Calculation: $09 + 2 + 2 + 3 = 16$

Toy hash: 16

» Block 3

Previous hash: 16

Transaction: Issue 1 book

Calculation: $16 + 3 + 1 + 3 = 23$

Toy hash: 23

Copy the three blocks onto your paper. Draw an arrow from each toy hash to the next block's previous-hash line.

ALTER AN EARLIER RECORD

1. Change Block 1 from "Receive 5 books" to "Receive 6 books."
2. Recalculate Block 1. Its toy hash changes from 09 to 10.
3. Compare the new Block 1 hash with the previous hash written in Block 2. They no longer match.
4. Change Block 2's previous hash to 10 and recalculate its toy hash. It changes from 16 to 17.
5. Compare the new Block 2 hash with the previous hash in Block 3. They no longer match.
6. Change Block 3's previous hash to 17 and recalculate its toy hash. It changes from 23 to 24.

REFLECT ON THE SIMULATION

Write brief responses to these questions:

- » What evidence revealed the change to Block 1?
- » Why did changing an earlier record affect later references?
- » Did the toy hash prove whether five or six books were actually received? Why or why not?
- » What would a person have to change to make every link match the altered record?
- » What important parts of a real blockchain did this paper activity leave out?



Important limitation of the simulation: This toy rule is a checksum-like class-room device. It has frequent collisions, is easy to reverse, and provides no security. A real blockchain uses secure cryptographic hash functions, network software, validation, digital signatures, and consensus rules. The exercise demonstrates linked references and tamper evidence only.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which sequence best describes the general path of a blockchain transaction?
 - a. Proposal, basic checking, selection into a proposed block, network agreement, and recording
 - b. Recording, deletion, advertising, and automatic proof of truth
 - c. Payment, bank approval, password recovery, and printing
 - d. Hashing, encryption, guaranteed acceptance, and permanent secrecy
2. Which statement best describes a cryptographic hash?
 - a. A reversible container that hides a message until a key opens it
 - b. A fixed-length result used to represent input data and help detect change
 - c. A guarantee that the input came from an honest person
 - d. A timestamp that proves when an outside event occurred
3. Why does changing information in an earlier block affect later hash references?
 - a. The later block contains a reference derived from the earlier block's data.
 - b. Every participant stores information in one physical computer.
 - c. Hashes automatically correct false information.
 - d. A block can contain only one transaction.

TRUE OR FALSE

- » If a transaction's hash matches the recorded hash, the match proves that every statement in the transaction was true and lawfully authorized.

SHORT EXPLANATION

- » In two or three sentences, explain the difference between saying a blockchain is tamper-evident and saying it is impossible to change.



SUMMARY AND PRACTICAL TAKEAWAYS

- » A transaction is a proposed change, not automatically an accepted fact.
- » Transactions pass through checks and network rules before becoming part of an accepted block.
- » A cryptographic hash produces a fixed-length digest that changes when the input changes.
- » Hashing is not the same as encryption and does not prove that the original information was true.
- » Blocks use hash-based references to connect the accepted history in sequence.
- » Altering an earlier block changes its hash and causes later references to stop matching unless the later chain is rebuilt and accepted.
- » Tamper-evident means a change leaves detectable evidence. Tamper-resistant means the system makes accepted alteration difficult. Neither means that change is impossible under every condition.

The practical skill is learning to ask two separate questions: Does the record show evidence of alteration, and was the information accurate and authorized when it entered the system?

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 the path from a proposed transaction to a recorded block in your own words.
- » Define a hash and describe how one block can use a hash to refer to an earlier block.
- » Explain why a changed record can cause later references to stop matching.
- » Distinguish tamper-evident or tamper-resistant from impossible to change.
- » Identify one thing a matching hash can show and one thing it cannot prove.
- » Connect careful wording to the critical-thinking or communication skills you are developing.

Your response should demonstrate your reasoning. You are not being asked to calculate a real cryptographic hash, create an account, open a wallet, purchase an asset, or conduct a transaction.



SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 6: Blocks, Transactions, and Hashes, 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 6 — [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, or other sensitive credentials.



UNDERSTANDING WEB3**LESSON 7: NODES, NETWORKS, AND CONSENSUS**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson explains technology. It does not recommend any network, company, product, or digital asset. It does not provide individualized financial, investment, legal, or tax advice. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.

OPENING GUIDANCE

Lesson 6 explained how transactions can enter blocks and how hashes can connect one block to the next. That explanation leads to another question: If many computers hold copies of a blockchain, how do they decide which new information belongs in the accepted record?

When I study a system that involves many participants, I find it useful to separate the people, the tools, and the rules. Who participates? What work does each participant perform? Which rules guide the group when messages arrive at different times or when participants disagree? I encourage you to use those questions throughout this lesson.

You do not need to become a miner, operate a validator, or run a node. Your objective is to understand the roles well enough to evaluate claims. Words such as decentralized and consensus can sound as if a network reaches perfect agreement without leadership, cost, or conflict. A responsible learner asks what the rules actually require, who has practical influence, and what tradeoffs follow.

PURPOSE AND ESSENTIAL QUESTION

Lesson 7 explains how a network of computers communicates, checks information, and reaches agreement under a set of rules.

Essential Question:

- » What can make a shared system trustworthy when no single participant controls the entire record?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define node and consensus mechanism.
- » Explain the problem consensus mechanisms are designed to address.
- » Compare proof of work and proof of stake at an introductory level.
- » Identify security, concentration, energy, speed, and participation tradeoffs.
- » Distinguish a node from a miner or validator.

KEY TERMS

NODE

Definition: A computer running software that connects to a blockchain network and performs one or more network functions, such as receiving, relaying, storing, or checking data.

Sample sentence: The node checked the proposed block against the network's rules before accepting it.

VALIDATOR

Definition: A participant or node authorized by a proof-of-stake or related system to propose, check, or vote on blocks according to the network's rules.

Sample sentence: The validator reviewed the proposed block and submitted a vote under the protocol.

MINER

Definition: A participant in a proof-of-work system that uses computing power to compete for the opportunity to propose a block.

Sample sentence: The miner searched for a valid proof of work that other nodes could verify.

CONSENSUS MECHANISM

Definition: The collection of rules, processes, and incentives that helps distributed participants agree on an accepted blockchain history.

Sample sentence: The consensus mechanism told nodes how to evaluate competing versions of the latest block.



PROOF OF WORK

Definition: A method used in some blockchain consensus systems in which miners perform computational work to compete for the right to propose blocks.

Sample sentence: Bitcoin uses proof of work as part of the process for adding blocks and selecting an accepted chain.

PROOF OF STAKE

Definition: A method used in some blockchain consensus systems in which validators commit value, called stake, and may face rewards or penalties as they propose or check blocks.

Sample sentence: In a proof-of-stake system, dishonest validator behavior may put staked value at risk.

MAIN LESSON

A BLOCKCHAIN IS ALSO A NETWORK

A blockchain is more than a chain of records. It is also a network of computers running software. Those computers exchange transactions, blocks, and other messages. Each computer that participates through the network software is commonly called a node.

Nodes do not all perform the same job. Depending on the network and configuration, a node may keep a full copy of the blockchain, keep only selected information, relay messages, check blocks, help an application read data, or participate directly in consensus. A computer does not become a miner or validator merely because it is a node. Miner and validator describe more specialized roles.

This distinction matters because statements such as “the nodes voted” may hide important details. Which nodes were eligible to participate? Did every node vote, or did only a selected group propose and attest to blocks? Could ordinary full nodes independently reject a block that violated protocol rules? Accurate analysis begins by identifying the actual role.

THE AGREEMENT PROBLEM

Imagine that several record keepers maintain copies of the same journal. New entries travel between them, but messages do not always arrive in the same order. Two proposed pages may appear at nearly the same time. One computer may go offline. Another may send incorrect information. A dishonest participant might create many false identities to appear more influential than one person should be.

The group needs rules for at least four questions:

1. Validity: What makes a transaction or block acceptable under the protocol?
2. Proposal: Who may propose the next block, and how is that participant selected?
3. Chain choice: If competing versions appear, which history should nodes follow?
4. Finality: When should participants treat a block as sufficiently settled that reversal is unlikely or prohibited by the rules?

A consensus mechanism addresses these questions through software rules, cryptography, communication, incentives, and sometimes penalties. It is not simply an informal vote. It also does not require every participant to agree at every instant. Networks may briefly have different views because messages take time to travel. The rules provide a method for those views to converge on an accepted history.

TEMPORARY DISAGREEMENT AND FINALITY

Suppose two valid block proposals reach different parts of a network almost simultaneously. Some nodes may see the first proposal before the second, while other nodes see them in the opposite order. For a short period, honest participants can hold different views of the newest accepted block.

The network's chain-choice rules tell nodes how to resolve that conflict as more information arrives. One proposed branch may become the accepted history while the other is left behind. This temporary division is often called a fork, although the word fork can also describe a deliberate change in software rules. Context determines which meaning applies.

Finality describes the point at which a network treats a block as settled under its design. Some systems provide increasing confidence as more blocks accumulate. Others use validator votes to mark a block final after defined conditions are met. Final does not mean that software, governance, or social decisions can never affect a network. It describes a technical status under the current protocol rules.

CONSENSUS DOES NOT PROVE TRUTH

Consensus can establish that network participants accepted a transaction under their technical rules. It cannot prove that every statement about the outside world was true.

Suppose an authorized organization records that a learner completed a course. Nodes may verify the format, digital signature, and other protocol conditions. The network may reach consensus that the record belongs in a block. Those checks do

not independently prove that the learner actually completed the work. The quality of outside information still depends on people, source records, authorization, audits, and accountability.

Consensus should therefore be understood as agreement about the network's record and state, not universal agreement about reality.

PROOF OF WORK AND THE MINER'S ROLE

In a proof-of-work system, miners compete by repeatedly performing a computational task. A miner assembles a proposed block and searches for a result that satisfies the network's difficulty rules. Finding a valid result can require substantial computation, while other nodes can check the result much more quickly.

When multiple valid chains exist, the protocol applies a chain-selection rule based on accumulated work. A block usually becomes harder to reverse as additional proof-of-work blocks build on top of it. Settlement is therefore often described in terms of confirmations and increasing confidence rather than an immediate promise that reversal is impossible.

Proof of work makes attempted manipulation costly because an attacker may need extensive computing equipment and energy to compete with the honest network. It also creates tradeoffs:

- » Mining can consume substantial electricity.
- » Specialized hardware and access to inexpensive energy may influence who can compete effectively.
- » Miners may combine resources in pools, creating concentration concerns.
- » Block times and confirmation practices can affect how quickly users treat a transaction as settled.
- » Security depends on the network's total honest computing power, software, incentives, and distribution—not on hashing alone.

Bitcoin is the best-known proof-of-work network. Ethereum also used proof of work historically, but it changed to proof of stake in 2022. That history is a reminder that a network's consensus design can change through an organized protocol upgrade.

PROOF OF STAKE AND THE VALIDATOR'S ROLE

In a proof-of-stake system, validators commit an asset as stake according to the network's rules. The system selects or assigns validators to propose blocks and to check or vote on proposed blocks. Honest participation may earn rewards. Cer-

tain provably dishonest behavior may lead to penalties, including the loss of some staked value, often called slashing.

Proof of stake replaces the proof-of-work competition for computing power with a security model built around committed value, validator messages, and penalties. It generally requires far less energy for block production than proof of work because validators are not racing through the same kind of repeated computational search.

Proof of stake also creates tradeoffs:

- » Greater stake may bring greater influence or a greater chance of selection, depending on the design.
- » Large holders, custodians, staking services, or coordinated operators may create concentration concerns.
- » Penalties can punish dishonest conduct, but software mistakes, configuration errors, or downtime may also create losses under some rules.
- » The details of proposer selection, voting, chain choice, and finality can be complex.
- » Participation requirements differ across networks and may include minimum stake, technical equipment, continuous operation, or delegation.

The phrase proof of stake describes a broad family of designs. Ethereum's system, BNB Smart Chain's system, and another proof-of-stake network may use different validator sets, voting procedures, finality rules, and penalties. Knowing the label is only the beginning of the analysis.

COMPARING THE TWO APPROACHES CAREFULLY

Proof of work and proof of stake aim to make dishonest control expensive, but they place the cost in different resources. Proof of work relies heavily on computing power and energy. Proof of stake relies on committed economic value and the threat of penalties.

Neither method automatically guarantees decentralization. A proof-of-work network can become concentrated among large mining operations or pools. A proof-of-stake network can become concentrated among large stakeholders, service providers, or a limited validator set. The important questions include how participation is distributed, how easily independent participants can verify the chain, how upgrades occur, and what happens when powerful actors coordinate.

Speed also requires careful wording. A consensus design may permit shorter block times or faster finality, but performance depends on the entire network architecture. Faster processing may involve tradeoffs in validator count, hardware requirements,

communication demands, or decentralization. The name of a consensus method alone does not prove that one network is faster, safer, cheaper, or more decentralized than another.

APPLIED EXAMPLE: BNB SMART CHAIN

As of July 20, 2026, BNB Chain's official documentation describes BNB Smart Chain as using Proof of Staked Authority, commonly shortened to PoSA. The design combines stake-based validator selection with an active set of validators that takes turns proposing and voting on blocks. Its rules also include penalties for conduct such as double signing, certain malicious votes, and extended downtime.

This example shows why labels require investigation. BNB Smart Chain uses stake, but its operation is not identical to Ethereum's proof-of-stake system. Its active validator design may support short block times and fast finality, while a limited block-producing set also raises questions about concentration and participation. Those are design tradeoffs to examine, not reasons to praise or reject the network automatically.

Mentioning BNB Smart Chain is an educational example. It is not an endorsement, an invitation to acquire BNB, or a request to operate a validator or conduct a transaction.

WHAT CREATES PRACTICAL TRUST

People sometimes describe blockchains as "trustless." A more careful explanation is that a blockchain can reduce dependence on one central record keeper by distributing verification across participants and enforcing shared rules. Trust does not disappear. It shifts.

Participants still rely on protocol design, software implementation, network communication, cryptography, economic incentives, operator behavior, governance, and access to independent verification. They may also rely on developers, hardware, internet providers, custodians, data sources, and legal institutions.

A shared system becomes more worthy of confidence when its rules are clear, independent participants can verify compliance, dishonest behavior is difficult or costly, failures are detectable, software is reviewed, and power is not dangerously concentrated. No single feature proves trustworthiness. Responsible evaluation looks at the system as a whole.

APPLIED SCENARIO: COMPETING RECORD KEEPERS

Seven community organizations maintain a shared record of donated textbooks. Each organization runs software that receives new entries and checks whether the submitting organization signed them correctly.

Two proposed blocks arrive close together. One records a delivery of 100 books. The other records 80. Both have a valid technical format, and each refers to a different source report. The organizations need a rule for choosing which proposed block becomes part of the shared history.

Under one possible design, participants who perform verifiable computational work compete to propose the block, and the network follows the valid chain with the most accumulated work. Under another design, selected participants place value at risk, propose or vote on a block, and may lose that value for provably conflicting conduct.

Reasoned conclusion: Either rule may help the network settle on one technical history. Neither rule proves whether 100 or 80 books actually arrived. The organizations still need delivery receipts, authorized submitters, correction procedures, and audits. Consensus can organize agreement about the record; outside evidence establishes whether the record reflects reality.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Shared rules can help independent computers converge on one accepted history.
- » Nodes can verify transactions and blocks instead of relying entirely on one record keeper.
- » Incentives and penalties can make certain dishonest behavior costly.
- » Multiple copies and independent verification can improve resilience.
- » Public protocols can make decision rules available for inspection.

IMPORTANT LIMITATIONS AND RISKS

- » Consensus does not prove that outside information was truthful or lawfully obtained.
- » Network delays, software defects, attacks, or configuration errors can disrupt agreement.
- » Mining power, stake, validator operation, software development, or infrastructure can become concentrated.
- » Proof of work may require substantial energy and specialized equipment.

- » Proof of stake may expose committed value to penalties and may concentrate influence among large stakeholders or services.
- » Governance decisions can change rules, divide communities, or create separate chains.

COMMON MISCONCEPTIONS

- » “Every node is a miner or validator.” Many nodes relay or verify information without proposing blocks.
- » “Consensus means every node agrees instantly.” Networks can have temporary disagreement and use rules to converge.
- » “Consensus proves the recorded claim is true.” It shows acceptance under network rules, not proof of every outside fact.
- » “Proof of work is secure because it uses hashes.” Its security depends on accumulated work, network distribution, incentives, software, and honest participation.
- » “Proof of stake is simply one person, one vote.” Voting weight and selection depend on the network’s protocol and stake rules.
- » “One consensus method is always superior.” Security, energy, speed, concentration, access, and governance involve tradeoffs.
- » “Trustless means no trust is required.” Trust shifts from one central keeper to a broader technical and social system.

OFFLINE EXERCISE: COMPARE THREE AGREEMENT RULES

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Imagine that seven record keepers maintain identical paper logs. Two conflicting entries arrive for the same delivery. The group must choose one entry for the next page.

RULE A: ONE COORDINATOR

One designated coordinator checks the entries and chooses the official version. Everyone copies that choice.

RULE B: PROOF-OF-EFFORT SIMULATION

Each proposed writer must complete a difficult paper puzzle. The first writer to produce a correct solution earns the opportunity to propose the page. The others



can check the solution quickly. Later pages build on the accepted page, and the group follows the valid history with the most accumulated puzzle work.

RULE C: STAKE-AT-RISK SIMULATION

Eligible writers place ten paper points at risk. The rules select one writer to propose the page. Other selected participants check it and record approval or rejection. A writer who signs conflicting pages loses the paper points under the exercise rules.

On separate paper, create four headings for each rule:

1. Who proposes the record?
2. What discourages dishonest behavior?
3. What concentration or participation risk exists?
4. What can the rule prove, and what can it not prove?

THEN ANSWER THESE QUESTIONS:

- » Which rule depends most directly on one trusted decision-maker?
- » Which rule makes repeated computational effort the scarce resource?
- » Which rule makes committed value and penalties the scarce resource?
- » How might power become concentrated under each rule?
- » Why would none of the three rules prove how many books actually arrived?
- » What additional evidence would the record keepers need?

Important limitation of the simulation: Real consensus mechanisms use software, cryptography, network messages, precise validity rules, proposer selection, chain-choice procedures, and incentives. Proof of work is not simply any difficult puzzle, and proof of stake is not simply a majority vote among people holding points. This activity compares broad resource and decision tradeoffs only.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes a blockchain node?
 - a. Every person who owns a digital asset
 - b. A computer running network software that performs one or more blockchain functions
 - c. Only the company that designed the blockchain
 - d. A paper record that cannot communicate with other systems



2. What problem is a consensus mechanism designed to address?
 - a. How distributed participants can agree on an accepted blockchain history
 - b. How to guarantee that every outside statement is true
 - c. How to eliminate all energy use and all concentration
 - d. How to provide individualized investment advice
3. Which comparison is most accurate?
 - a. Proof of work uses committed stake, while proof of stake uses only electricity.
 - b. Proof of work uses computational effort, while proof of stake uses committed value and validator rules.
 - c. Both systems require every node to be a professional miner.
 - d. Both systems prove that outside records are accurate.

TRUE OR FALSE

- » Every node on a blockchain network necessarily proposes blocks and participates directly as a miner or validator.

SHORT EXPLANATION

- » In two or three sentences, explain why reaching consensus about a blockchain record does not prove that every outside fact in the record is true.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A node is a computer running blockchain network software, but nodes can perform different roles.
- » Miners are block-producing participants in proof-of-work systems; validators perform defined roles in proof-of-stake or related systems.
- » A consensus mechanism helps distributed participants evaluate blocks, select an accepted history, and manage disagreement.
- » Proof of work makes computing power and energy central to block competition.
- » Proof of stake makes committed value, validator selection, voting, rewards, and penalties central to its security model.
- » Both approaches involve security, concentration, speed, energy, access, and governance tradeoffs.
- » Consensus establishes agreement under network rules; it does not independently prove outside truth.



The practical skill is learning to ask who participates, what each participant verifies, how block producers are selected, how competing histories are resolved, and where power could become concentrated.

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 a node and distinguish it from a miner or validator.
- » Explain the problem a consensus mechanism is designed to address.
- » Compare proof of work and proof of stake in your own words.
- » Identify one strength and one tradeoff associated with each approach.
- » Explain why consensus about a record does not prove every outside fact is true.
- » Describe what would make you trust a shared system when no single participant controls the entire record.
- » Connect this lesson to the critical-thinking, communication, or self-directed-learning skills you are developing.

Your response should demonstrate your reasoning. You are not being asked to operate a node, mine a block, stake an asset, create an account, open a wallet, purchase an asset, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 7: Nodes, Networks, and Consensus, 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 7 — [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, or other sensitive credentials.



UNDERSTANDING WEB3

LESSON 8: COMPARING BLOCKCHAIN NETWORKS AND UNDERSTANDING LAYERS

A Prison Professors Self-Directed Course

Estimated time: 70–105 minutes

Educational Boundary:

This lesson compares technical systems for educational purposes. It does not recommend any network, company, product, or digital asset. It does not provide individualized financial, investment, legal, or tax advice. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.

OPENING GUIDANCE

Lessons 5 through 7 introduced the basic structure of a blockchain, the relationship among blocks, transactions, and hashes, and the way nodes follow rules to reach agreement. We can now use those foundations to compare different networks.

When I compare systems, I try to avoid beginning with a conclusion. I begin with questions. What problem is the system designed to address? Who maintains it? What rules does it follow? What does it depend on? What benefits might it provide, and what tradeoffs come with those benefits?

This method is especially important in Web3 because a familiar name, a high price, or a label such as Layer 1 or Layer 2 can sound more informative than it really is. A label may help us organize an explanation, but it cannot replace careful analysis. I encourage you to practice separating the network from its native asset, the base layer from the systems connected to it, and technical claims from promotional claims.

PURPOSE AND ESSENTIAL QUESTION

Lesson 8 demonstrates that blockchain networks make different design choices and introduces the common language of Layer 1, Layer 2, and application layers.

Essential Question:

- » What criteria should a careful learner use to compare blockchain networks, and when does a layer label clarify or oversimplify the system?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Compare Bitcoin, Ethereum, BNB Smart Chain, and a connected scaling system using consistent criteria.
- » Distinguish a blockchain network from its native asset.
- » Explain Layer 1 as a base blockchain network and Layer 2 as a system built on or connected to a base network for defined purposes.
- » Explain why Layer 3 does not have one universal meaning.
- » Evaluate network and layer claims without treating popularity, price, speed, or a label as proof of quality.

KEY TERMS

BLOCKCHAIN NETWORK

Definition: A group of connected computers running compatible rules and software to exchange information, validate activity, and maintain a shared blockchain record.

Sample sentence: The blockchain network continued processing valid transactions even though one node went offline.

NATIVE ASSET

Definition: A digital asset built into a blockchain protocol and commonly used for functions such as paying network fees or supporting network security.

Sample sentence: Ether is the native asset of Ethereum, but ether and the Ethereum network are not the same thing.

LAYER 1

Definition: A base blockchain network that maintains its own ledger, consensus rules, and transaction history.

Sample sentence: Bitcoin, Ethereum, and BNB Smart Chain can each be examined as a Layer 1 network.

LAYER 2

Definition: A system built on or connected to a Layer 1 that processes or organizes activity and relies on that base network in a defined way.

Sample sentence: A Layer 2 may group transactions before sending information to its Layer 1.

APPLICATION LAYER

Definition: The programs and services through which people or organizations use blockchain-related functions.

Sample sentence: A ticketing program may operate at the application layer while relying on one or more blockchain networks underneath.

SCALABILITY

Definition: A system's ability to handle greater demand while maintaining acceptable performance, cost, security, and reliability.

Sample sentence: A design that processes more transactions may improve scalability but still introduce other tradeoffs.

FINALITY

Definition: The point at which a network treats a transaction or block as settled under its rules.

Sample sentence: A comparison of networks should explain how each system reaches finality instead of using the word fast by itself.

MAIN LESSON

COMPARE SYSTEMS, NOT SLOGANS

Blockchain networks do not all pursue the same goals or make the same design choices. One may emphasize resistance to control and a narrow set of functions. Another may emphasize general-purpose programs. Another may prioritize lower fees or shorter block times by using a smaller or differently selected validator group. A connected scaling system may move part of the work away from a base network and later submit data, proofs, or results back to it.

Because the designs differ, a fair comparison needs consistent questions. Comparing one network's speed with another network's market price would mix unrelated measurements. Comparing advertised maximum capacity with observed ordinary use would also be misleading. The learner's task is to decide what is being measured, under what conditions, and at what cost.

A useful comparison begins with at least seven criteria:

1. Purpose: What problem is the system designed to address?
2. Record and consensus: Who maintains the ledger, and how does the system accept new history?
3. Participation: Who can run a node, produce blocks, validate activity, or influence upgrades?
4. Performance and cost: What demand can the system handle, and what resources or fees are required?
5. Settlement: How and when does the system treat activity as final?
6. Programmability: What kinds of transactions, programs, or applications does the system support?
7. Dependencies and governance: What other networks, operators, bridges, data sources, companies, or decision processes does the system rely on?

These criteria do not produce one automatic winner. They reveal tradeoffs and help a learner match a system's design to a particular use.

SEPARATE THE NETWORK FROM THE ASSET

People often use a network name and an asset name as if they mean the same thing. They do not. Bitcoin can refer to the network and protocol, while bitcoin or BTC can refer to the network's native asset. Ethereum is a network and computing platform; ether or ETH is its native asset. BNB Smart Chain is a blockchain network; BNB is the native asset used for fees and other protocol functions in the BNB Chain ecosystem.

This distinction matters because a network can continue operating while the market price of its native asset changes. A price chart does not explain the network's consensus design, node distribution, software quality, governance, or usefulness. In the other direction, a technically capable network does not prove that its native asset will rise in price or suit any person's financial circumstances.

A responsible comparison can discuss how a native asset functions without making a recommendation to acquire it. The network is the system. The native asset is one component within that system.

LAYER 1: THE BASE RECORDKEEPING NETWORK

A Layer 1 is a base blockchain. It maintains the authoritative ledger under its own consensus rules. Nodes receive and check transactions and blocks. Miners or validators perform specialized roles according to the design. The Layer 1 also defines how fees are paid, how finality is reached, and how protocol changes occur.

Bitcoin, Ethereum, and BNB Smart Chain are different Layer 1 examples. Calling all three Layer 1 networks does not mean they are identical. Bitcoin uses proof of work and was introduced as a peer-to-peer electronic cash system. Ethereum uses proof of stake and supports general-purpose smart contracts. BNB Smart Chain uses Proof of Staked Authority and supports applications compatible with the Ethereum Virtual Machine. Each system has different participants, security assumptions, governance practices, performance characteristics, and concentration questions.

The Layer 1 label therefore answers only one question: Is this the base blockchain in the relationship being described? It does not answer whether the system is more decentralized, secure, useful, or valuable than another system.

LAYER 2: CONNECTED SCALING WITH A DEFINED DEPENDENCY

A Layer 2 handles some activity in connection with a Layer 1. The general purpose may be to improve scale, cost, speed, privacy, or another function. A Layer 2 might collect many transactions, process them separately, and later send data or results to the base network. The exact security and settlement relationship varies by design.

The phrase built on top of can be useful, but it is only an image. Computers do not sit physically on one another. The important questions are technical: What information goes to the Layer 1? Who operates the Layer 2? How can an incorrect result be challenged or rejected? Where is transaction data available? How do users move information or assets between systems? What happens if the Layer 2 operator stops working?

Not every separate chain connected by a bridge should automatically be called Layer 2. Some connected chains use their own consensus and security rather than deriving security from the base network. Different communities also apply the label differently. A careful explanation states the dependency instead of relying on the label alone.

Layer 2 designs can increase capacity or reduce ordinary transaction cost, but they may add complexity. Users may depend on sequencers or other operators, bridges, proof systems, challenge periods, data-availability arrangements, and upgrade controls. Moving work away from the base layer changes where trust, risk, and responsibility appear; it does not eliminate them.

APPLICATION LAYER AND THE VARIABLE MEANING OF LAYER 3

Applications and services help people use the underlying networks. A decentralized application may combine a user interface, smart contracts, outside data, storage, and ordinary web services. The application layer is where a technical system becomes a tool for a particular purpose, such as tracking credentials, coordinating a community project, or managing digital records.

An application is not automatically decentralized in every part merely because one smart contract uses a blockchain. Its website, administrators, data sources, keys, hosting, or upgrade process may remain concentrated. Comparing applications therefore requires questions about both the blockchain components and the surrounding service.

The term Layer 3 requires special care because it does not have one universal definition. One source may use it for an application-specific network built on a Layer 2. Another may mean an interoperability or service layer. Another may use Layer 3 as another name for the application layer. Whenever the term appears, ask the writer to define it. The definition and dependency matter more than the number.

A NEUTRAL COMPARISON OF THREE LAYER 1 NETWORKS

Bitcoin, Ethereum, and BNB Smart Chain provide a useful introductory comparison when the same criteria are applied to each.

Bitcoin: The original design describes a peer-to-peer electronic cash system. The network uses proof of work, and BTC is its native asset. Its design emphasizes a publicly verifiable transaction history and resistance to changing confirmed history through accumulated computational work. Tradeoffs include substantial energy use, confirmation time, and a more limited base-layer programming model than general-purpose smart-contract platforms.

Ethereum: Ethereum is a general-purpose blockchain network for transactions and smart contracts. It uses proof of stake, and ETH is its native asset. Its programmability supports many applications and token standards. Tradeoffs can include demand-driven fees, application and smart-contract risk, protocol complexity, and dependencies introduced by scaling systems and services.

BNB Smart Chain: BNB Smart Chain is an Ethereum-compatible blockchain network using Proof of Staked Authority, and BNB is its native asset for network functions such as fees. Its design supports short block times and application compatibility. Its active validator and block-production design also makes validator selection, stake concentration, governance, and operational influence important comparison questions.

These summaries are starting points, not verdicts. Terms such as secure, fast, decentralized, and scalable need evidence and a defined measurement. Each network can change through software upgrades, governance decisions, participant behavior, and changing demand.



APPLIED EXAMPLE: BNB SMART CHAIN AND OPBNB

As of July 20, 2026, BNB Chain's official documentation describes BNB Smart Chain as a base blockchain network and opBNB as a Layer 2 scaling solution for BNB Smart Chain built with the OP Stack. This gives us a practical layer relationship to examine.

BNB Smart Chain maintains the base ledger and consensus under its Layer 1 rules. opBNB processes activity in a connected environment intended to increase capacity and reduce cost for certain uses. Applications can then operate through opBNB or interact directly with BNB Smart Chain, depending on their design.

The label Layer 2 does not complete the evaluation. A careful learner would still ask who orders transactions, what data and results are posted to BNB Smart Chain, how errors are detected, how withdrawals or cross-system messages work, what upgrade controls exist, and what happens during an outage. The answers may change as the software develops, so current project documentation must be checked before publication or use.

This example is educational. It is not an endorsement of BNB Smart Chain, opBNB, BNB, or any application. No learner needs to acquire an asset, create a wallet, connect to a network, or conduct a transaction.

TRADEOFFS MOVE; THEY DO NOT DISAPPEAR

Layered designs can divide work among systems with different strengths. A base layer may emphasize security and independent verification. A connected layer may process more activity or provide specialized features. An application may make the technology easier to use.

The arrangement can also distribute risk across more components. A user may depend on the base network, the Layer 2 operator or validator set, a bridge, a data-availability system, smart contracts, an application interface, and people who control upgrades. Failure at any important point can affect the experience or outcome.

For that reason, the best comparison question is rarely Which network is best? A better question is Which design fits this purpose, under these conditions, with which benefits, costs, dependencies, and risks? That question encourages judgment instead of loyalty to a brand or label.

APPLIED SCENARIO: THE "LAYER 3" CREDENTIAL PROPOSAL

A community organization receives a proposal for a digital credential system. The vendor says the product is a Layer 3 application and therefore must be faster, safer, and more decentralized than every Layer 1 or Layer 2 alternative.

The proposal does not define Layer 3. It does not identify the base network, explain where records are stored, state who can change the software, or describe what happens if the vendor closes. It provides a chart showing transaction speed but does not explain the testing conditions or security assumptions.

Reasoned response: The organization should not accept the layer label as proof. It should ask the vendor to map every component: application, connected network, base network, operators, data storage, keys, upgrade controls, fees, and recovery process. It should compare the proposal with non-blockchain alternatives using the same requirements. The label may become useful after the dependencies are clear, but it cannot replace evidence.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF A LAYERED MODEL

- » Separating base recordkeeping, scaling, and application functions can make a complex system easier to analyze.
- » Layer 2 systems may increase capacity or reduce ordinary transaction cost for some uses.
- » Application layers can turn technical functions into tools that serve a specific purpose.
- » Multiple designs allow builders to choose among different performance, security, privacy, and programmability tradeoffs.
- » Consistent comparison criteria can help learners evaluate claims without relying on price or popularity.

IMPORTANT LIMITATIONS AND RISKS

- » Layer terminology is descriptive rather than universal, especially for Layer 2 boundaries and Layer 3.
- » A connected system may introduce operators, bridges, proof systems, data services, or upgrade controls that become new points of dependence.
- » Faster or cheaper processing may involve tradeoffs in decentralization, security, data availability, or finality.
- » Native-asset prices can distract from technical evaluation and can change independently of network quality.
- » Software defects, governance disputes, concentrated control, misleading benchmarks, and incompatible upgrades can affect any layer.

- » Applications can remain highly centralized even when they use a public blockchain.

COMMON MISCONCEPTIONS

- » “A network and its native asset are the same thing.” The asset is one component of the network’s economic and security design.
- » “Layer 2 always means a separate blockchain with identical security to Layer 1.” Designs and dependencies differ; the relationship must be explained.
- » “Layer 3 is a universally agreed technical category.” Sources use the term in different ways.
- » “A higher layer number means better technology.” Layer numbers describe a relationship, not a quality score.
- » “The fastest network is automatically the best network.” Performance must be compared with security, cost, participation, reliability, and purpose.
- » “A popular or expensive native asset proves that its network is useful or safe.” Price and popularity do not establish technical quality.
- » “Moving work to another layer removes trust.” Trust and risk usually shift to different components and operators.

OFFLINE EXERCISE: BUILD A NEUTRAL COMPARISON MATRIX

Estimated time: 25–30 minutes

Materials: Separate paper and a pencil.

Create a comparison matrix on separate paper. Use these five rows:

- » Bitcoin
- » Ethereum
- » BNB Smart Chain
- » opBNB
- » The hypothetical credential application from the applied scenario

CREATE THESE SIX COLUMN HEADINGS:

1. Category: Layer 1, Layer 2, application layer, or unclear
2. Purpose: What is the system designed to do?
3. Dependencies: What network, participants, operators, or services does it rely on?
4. Possible benefit: What strength might the design provide?

5. Important tradeoff or risk: What cost, limitation, or concentration question matters?
6. Missing information: What would you need to verify before reaching a conclusion?

Complete every row using this lesson. When information is incomplete, write unknown—needs verification instead of guessing.

Then write a short response to these questions:

- » Which examples are base networks?
- » Which example depends on a base network as a scaling system?
- » Which example is mainly an application or service?
- » Why would price be a poor column for comparing technical design?
- » Which two criteria would matter most for a credential system, and why?
- » Where might control or failure become concentrated in each example?

Important limitation of the exercise: This matrix simplifies systems that contain many components and can change over time. It helps organize questions; it does not provide a complete security audit or prove that one system is superior.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best distinguishes a blockchain network from its native asset?
 - a. The network is the shared technical system; the native asset is one component used within that system.
 - b. The native asset owns every node in the network.
 - c. The network is only the asset's market price.
 - d. There is no difference between the two terms.
2. Which description of Layer 1 is most accurate?
 - a. Any website that displays blockchain information
 - b. A base blockchain network with its own ledger and consensus rules
 - c. A quality score assigned to the most popular asset
 - d. A private key stored in a wallet
3. Which question is most useful when evaluating a claimed Layer 2 system?
 - a. Does its name contain the number two?



- b. Is its native asset rising in price today?
- c. What does it process, what does it post to the base network, and what security dependencies does it introduce?
- d. Does its advertisement call it the fastest?

TRUE OR FALSE

- » The term Layer 3 has one universal definition that every blockchain project uses in the same way.

SHORT EXPLANATION

- » In three or four sentences, explain why a higher layer number, faster advertised speed, or more expensive native asset does not by itself prove that a system is better.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Blockchain networks should be compared using consistent criteria, including purpose, consensus, participation, performance, finality, programmability, dependencies, and governance.
- » A network and its native asset are related but different.
- » A Layer 1 is a base blockchain network that maintains its own ledger and consensus rules.
- » A Layer 2 processes or organizes activity in a defined relationship with a Layer 1.
- » Applications and services interact with networks but may include both decentralized and centralized components.
- » Layer 3 does not have one universal meaning; every use should be defined.
- » Bitcoin, Ethereum, and BNB Smart Chain are Layer 1 networks with different designs and tradeoffs.
- » Official documentation currently describes opBNB as a Layer 2 scaling system connected to BNB Smart Chain.
- » Layer labels, speed claims, popularity, and asset prices do not replace evidence.

The practical skill is learning to map a system before judging it: identify the base record, connected layers, applications, participants, dependencies, benefits, and risks.



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 why blockchain networks should be compared with consistent criteria.
- » Distinguish a blockchain network from its native asset.
- » Define Layer 1, Layer 2, and the application layer in your own words.
- » Explain why Layer 3 must be defined each time it is used.
- » Compare two examples from the lesson using the same criteria.
- » Identify one possible benefit and one important tradeoff of a layered system.
- » Describe how you would respond to a claim that one network is best because it is faster, more popular, or has a higher-priced asset.
- » Explain what criteria you would use to decide whether a layer label clarifies or oversimplifies a system.
- » Connect the comparison process to the critical-thinking, communication, or self-directed-learning skills you are developing.

Your response should demonstrate your reasoning. You are not being asked to create an account, open a wallet, purchase an asset, connect to a network, use an application, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 8: Comparing Blockchain Networks and Understanding Layers, 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 8 — [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, or other sensitive credentials.

UNDERSTANDING WEB3

SECTION 2 REVIEW: BLOCKCHAIN FOUNDATIONS

A Prison Professors Self-Directed Course

Estimated time: 60–90 minutes

Educational Boundary:

This review provides general education about technology and preparation. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, product, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this review.

REVIEW PURPOSE

You have completed Lessons 5 through 8 of Understanding Web3. This review gives you a place to pause, strengthen your vocabulary, and connect the components of a blockchain before moving into the next section.

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, study the relevant passage, and revise your response. That cycle can help you develop the habits of a self-directed learner.

THE REVIEW COVERS:

- » The purpose, structure, possible benefits, and limitations of a blockchain.
- » The path from a proposed transaction to a recorded block, including the role of cryptographic hashes.
- » Nodes, consensus mechanisms, proof of work, proof of stake, finality, and the limits of technical agreement.
- » How to distinguish a blockchain network from its native asset and compare Layer 1, Layer 2, and application-layer designs.

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 compare alternatives.
- » 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, 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 complete.

PART 1: KNOWLEDGE QUESTIONS

MULTIPLE CHOICE

1. Which statement best describes a blockchain?
 - a. A system that guarantees every recorded statement is true
 - b. A shared digital ledger in which records are grouped into blocks, linked in order, and maintained according to a network's rules
 - c. A private password that authorizes every type of online transaction
 - d. A label that applies to every conventional database
2. Which sequence best describes the general path of a blockchain transaction?
 - a. Proposal, basic checking, selection into a proposed block, network agreement, and recording
 - b. Recording, deletion, advertising, and automatic proof of truth
 - c. Payment, bank approval, password recovery, and printing
 - d. Hashing, encryption, guaranteed acceptance, and permanent secrecy
3. Which statement best describes a cryptographic hash?
 - a. A reversible container that hides a message until a key opens it
 - b. A fixed-length result used to represent input data and help detect change
 - c. A guarantee that the input came from an honest and authorized person
 - d. A timestamp that independently proves when an outside event occurred
4. Which statement accurately distinguishes a node from a miner or validator?
 - a. Every node must propose a block.



- b. A node may receive, relay, store, or check data without serving as a miner or validator.
 - c. A miner or validator cannot run network software.
 - d. The terms node, miner, and validator always describe the same role.
- 5. What problem is a consensus mechanism designed to address?
 - a. How distributed participants can agree on an accepted blockchain history
 - b. How to prove that every statement about the outside world is true
 - c. How to eliminate all costs, delays, and concentration risks
 - d. How to make every network use the same rules
- 6. Which statement most accurately compares proof of work and proof of stake?
 - a. Proof of work uses computational work, while proof of stake uses committed value and possible penalties; both involve tradeoffs.
 - b. Proof of work guarantees decentralization, while proof of stake guarantees speed.
 - c. Proof of stake gives every person one equal vote, while proof of work has no participation rules.
 - d. The two terms describe identical systems with different names.
- 7. Which question is most useful when evaluating a system described as a Layer 2?
 - a. Does its name include the number two?
 - b. Is its related asset increasing in price?
 - c. Which Layer 1 does it depend on, what information does it post there, and what new dependencies does it introduce?
 - d. Does an advertisement describe it as the fastest network?

TRUE OR FALSE

- 1. A network may reach consensus that a transaction belongs in its record without proving that every outside claim in the transaction is true.
- 2. The term Layer 3 has one universal definition that every blockchain project uses in the same way.

SHORT EXPLANATION

- » In three to five sentences, explain why neither a matching hash nor network consensus proves that the information entering a blockchain was truthful and properly authorized. Identify one type of outside evidence or process that could help establish accuracy.



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. Blockchain
- b. Ledger
- c. Transaction
- d. Hash
- e. Tamper-evident
- f. Node
- g. Consensus mechanism
- h. Proof of work
- i. Proof of stake
- j. Native asset
- k. Layer 1
- l. Layer 2

DEFINITIONS

- 1. A proposed action or change that a system may verify and add to its record; it does not have to involve money.
- 2. A base blockchain network that maintains its own ledger, consensus rules, and transaction history.
- 3. An organized record of transactions, events, balances, or other changes.
- 4. A method in which validators commit value and may face rewards or penalties as they propose or check blocks.
- 5. A shared digital ledger in which records are grouped into blocks, linked in order, and maintained according to a network's rules.
- 6. A fixed-length result produced when a hash function processes data and designed to make changes to the input detectable.
- 7. A computer running software that connects to a blockchain network and performs one or more network functions.
- 8. A digital asset built into a blockchain protocol and commonly used for functions such as paying network fees or supporting network security.



9. Designed so that an unauthorized or unexpected change leaves evidence that can be detected.
10. A method in which miners perform computational work to compete for the opportunity to propose blocks.
11. The collection of rules, processes, and incentives that helps distributed participants agree on an accepted blockchain history.
12. A system built on or connected to a Layer 1 that processes or organizes activity and relies on that base network in a defined way.

PART 3: APPLIED SCENARIO — A SHARED LEARNING RECORD

Five community organizations offer educational programs. They want to create a shared record of course completions while keeping sensitive learner information outside the shared system. A technology provider proposes the following design:

- » An authorized organization submits a digitally signed completion record. The proposal is treated as a transaction.
- » Software checks the transaction's format and signature. Accepted transactions are grouped into blocks.
- » Each new block contains a hash-based reference to the previous block.
- » Each organization operates a node that keeps a copy of the record and checks blocks against shared rules.
- » Selected validators commit value under the system's rules, propose or vote on blocks, and may face penalties for provably conflicting conduct.
- » The provider calls the system a Layer 2, but its proposal does not identify the Layer 1, explain what information will be posted to that base network, or describe what happens if the connection fails.

The provider's promotional materials state: "Our blockchain is immutable. Consensus proves every completion record is genuine. Because the system is fast and its native asset has a high price, it is the best design for educational credentials."

SCENARIO QUESTIONS

1. Identify the transaction, block, hash reference, nodes, and validators described in the proposal. Explain the function of each.
2. What could the hash-based reference help the organizations detect? What could it not prove about a learner's course completion?
3. What could consensus establish about the shared record? What outside facts would still require evidence, authorization, or review?



4. Which details suggest that the proposal uses a proof-of-stake approach? What additional information would you request before evaluating its security and concentration risks?
5. What information would the provider need to supply before the organizations could evaluate the Layer 2 label and its dependencies?
6. Compare the proposed blockchain with the alternative of one trusted organization maintaining a conventional database. Identify one possible benefit and one limitation of each design. Then recommend the next step the organizations should take before choosing, and explain your reasoning.

COMPLETION CHECK

Before moving to Section 3, ask yourself whether you can:

- » Explain a blockchain using the ideas of a ledger, transactions, blocks, links, and a network.
- » Describe how a hash can help reveal a change without proving that the original information was true.
- » Distinguish a node from a miner or validator and explain the purpose of consensus.
- » Compare proof of work and proof of stake without assuming that either method removes every risk.
- » Distinguish a network from its native asset and evaluate Layer 1 and Layer 2 claims by examining evidence and dependencies.

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

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 2 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 2 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, or other sensitive credentials.



UNDERSTANDING WEB3**LESSON 9: CRYPTOCURRENCIES, COINS, AND TOKENS**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson provides general education about technology and risk. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any network, company, product, token, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.

OPENING GUIDANCE

Lesson 8 separated a blockchain network from its native asset. That distinction prepares us to examine a wider category: digital assets. People often use words such as cryptocurrency, coin, and token as if they mean exactly the same thing. In practice, speakers, projects, regulators, and technical documents may use those labels differently.

I encourage you to look beyond the label. Ask what the asset is, where its record exists, how it was created, what function it performs, what rights it provides, who can change its rules, and what important risks remain. A familiar name or a confident explanation does not answer those questions.

Some participants may wonder why these distinctions matter if they cannot access a blockchain, create an account, or use a digital asset. Later in this lesson, we will examine how an independent Web3 community used BNB Smart Chain, a token, a smart contract, and a public treasury address to support the Prison Professors mission. That real example shows why the vocabulary matters. It also shows why inspiration should be accompanied by careful questions.

This lesson will not ask you to predict a price or decide whether to acquire an asset. The objective is to build a classification and evaluation process. That process can help you separate a technical function from a promotional claim and explain what information is still missing.

PURPOSE AND ESSENTIAL QUESTION

Lesson 9 explains the difference between a blockchain's native asset and tokens created through a blockchain platform. It also introduces a disciplined way to evaluate claims about digital assets.

Essential Question:

- » What questions should a careful learner ask before accepting a claim about a digital asset?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Distinguish cryptocurrency, coin, token, and native asset using the course definitions.
- » Explain several functions a digital asset may perform without treating those functions as proof of value.
- » Identify the rights, restrictions, control points, and missing information associated with a hypothetical asset.
- » Explain why a utility label does not guarantee usefulness, price, liquidity, or legal treatment.
- » Identify volatility, limited liquidity, fraud, technical failure, and regulatory uncertainty as material risks.

KEY TERMS

CRYPTOCURRENCY

Definition: A broad label for digital assets that use cryptography and blockchain or related distributed-ledger systems to record or transfer value. Usage varies, so the speaker's meaning should be defined.

Sample sentence: The word cryptocurrency described the broad category, but the learner still asked whether the asset was a native coin or a token on another network.

COIN

Definition: In this course, a digital asset that is native to its own blockchain network and operates under that network's protocol rules.

Sample sentence: The network used its native coin to pay transaction fees.



TOKEN

Definition: In this course, a digital asset created and recorded through code on an existing blockchain platform rather than serving as that platform's native asset.

Sample sentence: The organization created a token through a smart contract on an existing blockchain.

NATIVE ASSET

Definition: A digital asset built into a blockchain protocol and commonly used for functions such as paying network fees or supporting network security.

Sample sentence: The native asset belonged to the base network, while many separate tokens operated through programs on that network.

UTILITY

Definition: A practical function or use that an asset is designed to support within a network, application, or service.

Sample sentence: The provider claimed that the token's utility was access to a digital learning service, but the learner asked whether the service was operating and whether access could be revoked.

LIQUIDITY

Definition: The ability to buy, sell, or exchange an asset without excessive delay or a large change in its price. Liquidity can vary across markets and over time.

Sample sentence: A displayed price did not prove liquidity because very few buyers or sellers might be available at that price.

MAIN LESSON

BEGIN WITH THE BROAD CATEGORY

A digital asset is a record of value, access, rights, or information represented in digital form. Some digital assets operate on blockchains, while others exist only in a company's conventional database. Not every digital point, credit, or electronic balance is a cryptocurrency or token.

For this course, cryptocurrency is the broad category for digital assets that rely on cryptography and blockchain or related distributed-ledger systems. A coin is the native asset of a blockchain. A token is created through code on an existing blockchain platform. This teaching model helps organize the concepts, but industry

usage is not perfectly consistent. A source may call a native asset a coin, a token, a cryptocurrency, or all three.

I encourage you to define the term before debating it. If two people use token differently, they may appear to disagree when they are describing the same technical object with different vocabulary.

A COIN BELONGS TO THE BASE PROTOCOL

A native coin or native asset is part of a blockchain's base design. The protocol defines how the asset is recorded and how it may be used. Common functions include paying transaction fees, rewarding participation, or supporting a proof-of-stake system.

Bitcoin is the native asset of the Bitcoin network. Ether is the native asset of Ethereum. BNB is the native asset used on BNB Smart Chain. These examples identify a relationship between an asset and a network; they do not recommend the asset or predict its price.

A coin's technical role does not make it safe or valuable. Network defects, governance decisions, market conditions, concentration, loss of access, fraud, and legal developments may still affect people who use or hold it.

A TOKEN USES AN EXISTING PLATFORM

A programmable blockchain can support code that creates and manages other digital assets. On Ethereum, the ERC-20 standard defines common functions for fungible tokens. BNB Smart Chain supports contract-based tokens commonly described as BEP-20 tokens. The code may track balances, transfers, total supply, permissions, or other rules.

The token depends on more than its own name. It may rely on the base network, a smart contract, developers, administrators, an issuer, an application, data providers, marketplaces, or legal agreements. A failure or decision at one of those points may affect the token.

A token may also include administrative powers. Depending on its code, an authorized party might pause transfers, create more units, destroy units, restrict certain addresses, or change connected services. Those powers may help correct problems or comply with obligations, but they may also concentrate control. A careful learner asks what powers exist, who holds them, and how their use is governed.

FUNCTION DOES NOT ESTABLISH VALUE OR RIGHTS

Digital assets can serve different functions. An asset may be used to:

- » Pay a network or application fee.
- » Participate in network security under defined rules.
- » Access a service, feature, membership, or digital resource.
- » Record voting power or participation in a governance process.
- » Represent points, rewards, or credits within a program.
- » Represent a claim or interest described in a separate agreement.

The function must be verified. A token that is advertised as providing access may depend on a service that does not yet exist. A governance token may provide only limited voting power, while a small group retains authority to override decisions. A token described as representing an asset may not create an enforceable ownership right unless the technical record and the governing agreement actually do so.

For that reason, identifying a function is only the beginning. The learner should ask what the holder can do, what the holder cannot do, who owes any obligation, what restrictions apply, and what evidence supports the claim.

THE UTILITY LABEL REQUIRES INVESTIGATION

The word utility describes a proposed use. It does not guarantee that the use is necessary, available, valuable, or lawful. It also does not guarantee that the asset will have buyers, maintain a price, or avoid regulation.

Suppose a project calls an asset a utility token because people may use it for future access to an educational platform. Important questions remain:

- » Does the platform exist and work?
- » Is the token necessary, or could the service use an ordinary account or payment system?
- » What exactly does one token permit the holder to do?
- » Can the issuer change the rules, supply, price, or access conditions?
- » Does the holder receive a contractual right, or only a technical ability under current code?
- » What happens if the organization, website, or development team stops operating?

I encourage learners to replace the question “Is it a utility token?” with “What verified utility does it provide, under whose rules, with what limitations?”



LIQUIDITY IS DIFFERENT FROM A DISPLAYED PRICE

Liquidity describes whether an asset can be exchanged without excessive delay or a large price change. A market screen may show the most recent trade, but that number does not prove that many buyers and sellers are available.

An asset with limited trading activity may have a large difference between the price buyers offer and the price sellers request. A person trying to sell may receive much less than the displayed price, may wait for a buyer, or may find no reliable market. A platform may also halt withdrawals or trading. Liquidity can disappear during stress, even when it appeared sufficient before.

This course does not ask participants to trade. The lesson uses liquidity as an example of why a claim about value requires more evidence than one price or one advertisement.

RISKS DO NOT DISAPPEAR WHEN AN ASSET HAS A PURPOSE

A digital asset can perform a real technical function and still involve serious risk. Material risks may include:

- » Volatility: The market price may change rapidly and unpredictably.
- » Limited liquidity: A holder may not be able to exchange the asset when expected or near a displayed price.
- » Fraud and misrepresentation: Promoters may invent partnerships, hide control, exaggerate demand, or promise returns that cannot be supported.
- » Technical risk: Code defects, network failures, compromised credentials, or administrative powers may cause loss or restriction.
- » Concentration and governance risk: A small group may control supply, upgrades, validation, markets, or decisions.
- » Regulatory uncertainty: Legal treatment can depend on jurisdiction, facts, rights, marketing, and how an asset is offered or used.

As of July 21, 2026, United States regulatory advisories continue to warn that digital-asset markets may involve volatility, illiquidity, fraud, hacking, platform failure, and limited remedies. This lesson does not classify any asset under law. A label such as coin or utility token does not settle whether a particular law applies.

APPLIED EXAMPLE: BNB SMART CHAIN

As of July 21, 2026, BNB Chain documentation describes BNB as the native utility token of BNB Smart Chain and identifies BNB as an asset used for transaction



fees. The same documentation distinguishes native BNB transfers from transfers of contract tokens such as BEP-20 tokens.

Under this course's teaching distinction, BNB functions as the native coin or native asset of BNB Smart Chain. A BEP-20 token is created through code operating on that existing network. Official documentation may still use the word token for BNB, which shows why labels should be defined rather than assumed.

This example does not establish that BNB or a BEP-20 token is useful, safe, liquid, or appropriate for any person. Each asset requires separate analysis of purpose, code, rights, control, market conditions, and risk.

A DISCIPLINED EVALUATION PROCESS

Before accepting a claim about a digital asset, organize the questions into six groups:

1. Technical identity: Is it a native asset, a token on another network, a database entry, or something else?
2. Function: What can the asset actually be used to do today?
3. Rights and restrictions: What does a holder receive, and what limits or obligations apply?
4. Control and dependencies: Who can create units, change rules, pause activity, operate the service, or influence decisions?
5. Evidence: Which official code, documentation, agreements, audits, or records support the claim?
6. Risks and alternatives: What could fail, what information is missing, and could a simpler system serve the same purpose?

That framework does not produce a guaranteed answer. It helps a learner explain what is known, what is claimed, and what must still be verified.

REAL-WORLD CASE STUDY: A WEB3 COMMUNITY SUPPORTS PRISON EDUCATION

WHY THIS STORY MATTERS TO ME

I served 26 years in federal prison. During those years, I did not have access to the tools that define today's digital economy. I could, however, read, write, study, ask questions, and document what I was learning. That pattern of self-directed learning helped me build credibility. After my release, relationships and opportunities opened because other people could see evidence of preparation.

That experience shapes the way I view Web3. I do not want participants to study vocabulary only to pass a knowledge check. I want them to see how learning can

PRISON PROFESSORS CHARITABLE CORPORATION

Prison Professors Charitable Corporation / 1205 BMC Drive / Suite #706 / Cedar Park, TX 78613
IRS 501c3 #85-2603315 / www.PrisonProfessors.org



prepare a person to recognize opportunities, communicate with new communities, evaluate claims, and contribute responsibly.

The Prison Professors Token provides a real example. It does not prove that every token is useful or that any person should acquire one. It shows how the concepts in this course can operate together in the world.

HOW I CAME TO KNOW CZ

Changpeng Zhao, widely known as CZ, is the founder of Binance, a global cryptocurrency exchange. I met him while he was going through his own challenges with the United States justice system. As he prepared for and then served a four-month sentence in federal prison, we communicated frequently. I assisted him as he worked on the manuscript that became *Freedom of Money*, and I later narrated the audiobook.

In the book, CZ wrote about his support for Prison Professors. He also provided resources that help us expand our mission of making educational materials available to people in prison without charge. Through the book and CZ's public support, people in many parts of the world learned about our work.

PEOPLE WE DID NOT KNOW RESPONDED TO THE WORK

After *Freedom of Money* was released in 2026, a group of people formed an independent Web3 community around the Prison Professors mission. Neither CZ nor I knew the organizers. They learned about the mission, decided that they wanted to participate, and used the BNB ecosystem to launch a token commonly identified by the symbol PP.

Neither CZ nor I created the token. Prison Professors did not organize, manage, or control the token project. The community website identifies it as an independent effort, not as an official Prison Professors product or endorsement. Preserving that distinction helps a careful learner understand that a token can refer to a person or mission without being controlled by that person or organization.

The community used a smart contract on BNB Smart Chain. Its website states that the system applies a 3 percent charge when trades occur and directs the resulting resources toward a public donation address. The website calls the charge a tax. In this course, transaction fee is the clearer term because the charge is created by program rules, not imposed by a government.

I find another lesson in the way this community formed. The organizers did not need to know me personally before they could evaluate the work. They could read about the mission, examine the record, and decide whether they wanted to help. A person in prison can begin building that kind of record now by learning, writing,

keeping promises, and documenting progress. No journal entry guarantees that a future employer, mentor, or supporter will respond. A sustained body of work can, however, give people who do not yet know you something meaningful to evaluate.

THE CASE CONTAINS SEVERAL KINDS OF DIGITAL ASSETS

The case becomes easier to understand when we separate its components:

1. BNB Smart Chain is the blockchain network. It provides the shared infrastructure that records transactions and executes the smart contract.
2. BNB is the network's native asset. It can be used for transaction fees under the network's protocol rules.
3. PP is a token created on that existing network. Its balances and transaction-fee logic depend on smart-contract code and the BNB Smart Chain.
4. WBNB is Wrapped BNB. It is a contract-based token representation of BNB that can interact with applications using the BEP-20 token standard.

This is why a treasury screen may show both native BNB and WBNB.

This one case therefore demonstrates the lesson's principal distinction: BNB is native to the base network, while PP and WBNB are tokens that use the network.

WHAT BSCSCAN AND TELEGRAM CAN SHOW

BscScan is a blockchain explorer, which is a public search tool for activity recorded on BNB Smart Chain. A person can enter a public address and view balances and transactions associated with that address. BscScan does not open the wallet or reveal its private key. It organizes information that the blockchain makes public.

Telegram is a messaging service that many online communities use for group announcements and discussions. The PP community uses a Telegram channel with an automated tracker that posts notices about transfers and maintains a running donation total. The tracker is a community communication tool; it is not the blockchain itself.

On July 21, 2026, a live BscScan screen supplied for this lesson showed the public treasury address holding more than 943 WBNB, along with a smaller native BNB balance. At approximately the same time, the community's Telegram tracker reported more than 943 BNB in cumulative donations. These figures describe related information in different ways: BscScan showed assets held at the public address at that moment, while the Telegram tracker reported a running total of transfers. The totals continue to change as transactions occur, and any dollar estimate changes with the market price of BNB.

I use a cold-storage arrangement for the treasury and have pledged to reserve these resources at least until summer 2027 while we build a responsible, mission-aligned

plan. I have also connected future use of the resources to reaching meaningful participation in Prison Professors programs.

The public ledger allows an observer to examine the address, balances, and transaction history without relying only on a private report. That transparency has practical value. It does not answer every question. A blockchain record does not prove how private keys are stored, who can authorize a future transfer, whether a public promise will be honored, how a nonprofit will account for the resources, or what the resources will be worth later. Those questions require policies, governance, documentation, and human accountability.

WHAT THIS CASE DOES AND DOES NOT DEMONSTRATE

The case demonstrates that a community can use a blockchain and smart contract to coordinate support across borders, automate a transaction-fee rule, and make treasury activity publicly visible. It also demonstrates that technology can connect people who may never enter a prison with a mission serving people inside prisons.

The case does not establish that PP, BNB, WBNB, or any other digital asset is safe, liquid, legally classified in a particular way, or appropriate for any person. It does not guarantee that community attention will continue or that a displayed market price can be obtained in a future transaction. The community's enthusiasm, the smart contract, the public treasury, and Prison Professors' stewardship are related but distinct parts of the system.

Reasoned conclusion: The Prison Professors Token fits this course's definition of a token because it was created through a smart contract on an existing blockchain. Its programmed transaction fee provides a real function: directing resources toward a public mission address. That function is meaningful, but it does not eliminate questions about control, security, liquidity, governance, legal treatment, or future use. A disciplined learner can appreciate the social impact while still asking careful questions.

A RECURRING EXAMPLE IN LATER LESSONS

We will return to this case as the course introduces wallets and public addresses, transaction flow, smart contracts, treasury governance, real-world applications, and transferable skills. Each later lesson will examine a different part of the case. Repeated study can help participants connect new vocabulary with one documented example while continuing to distinguish public evidence from claims that require human judgment.

WHY THIS MATTERS WHILE YOU ARE IN PRISON

You do not need internet access, a wallet, or money to learn from this case. You can identify the network, distinguish the native asset from the tokens, explain what the smart contract is intended to do, identify what the blockchain can verify, and list what still depends on people.

Those are transferable skills. Employers, partners, and community members value people who can study unfamiliar systems, separate evidence from claims, communicate clearly, and exercise judgment. Every thoughtful journal entry can become part of the record you are building.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » A native asset can support fees, incentives, or network security under protocol rules.
- » A token can represent access, participation, points, or other functions through programmable rules.
- » Shared technical standards can help applications recognize and interact with compatible tokens.
- » Public records and code may allow independent review of some supply, transfer, or permission rules.

IMPORTANT LIMITATIONS AND RISKS

- » A technical record does not prove that an issuer's outside claim is truthful or enforceable.
- » A useful function does not guarantee market value, liquidity, safety, or legal compliance.
- » Smart contracts, administrators, platforms, or connected services may fail or change.
- » Prices can be volatile, markets can become illiquid, and fraud can cause permanent loss.
- » Legal and regulatory treatment may change or differ across jurisdictions and circumstances.

COMMON MISCONCEPTIONS

- » "Coin and token always mean exactly the same thing." Usage varies; define the term and examine the technical structure.

- » “A utility token must be useful.” The proposed service may be limited, unnecessary, unfinished, or unavailable.
- » “A displayed price proves I can sell at that price.” A market may have limited liquidity or unreliable withdrawals.
- » “A real use guarantees a rising price.” Function and market price are different questions.
- » “Blockchain code guarantees legal ownership.” Rights may depend on agreements, law, authorization, and facts outside the blockchain.
- » “Native means safe.” A native asset can still involve technical, governance, market, fraud, and legal risks.

OFFLINE EXERCISE: CLASSIFY ASSETS AND IDENTIFY GAPS

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

For each hypothetical item below, write four headings: classification, function, control or dependency, and missing information.

1. BaseUnit: Built into a blockchain’s protocol. It pays transaction fees and may be committed by validators under the network’s rules.
2. CoursePass: Created by a smart contract on BaseUnit’s network. The provider says ten units permit access to one course, but it can change the access policy.
3. StudyPoints: Recorded only in one school’s conventional database. They cannot move to a blockchain address or another organization.
4. CommunityVote: Created on an existing blockchain. Holders may vote on proposals, but the development company can reject any vote.
5. FutureSkill: Advertised as a utility token for a service planned for next year. One recent trade is displayed, but the number of buyers and sellers is unknown.

FOR EACH ITEM:

- » Classify it as a native coin or asset, a token, a conventional database entry, or unknown—needs verification.
- » State the function that the description supports without adding a promise.
- » Identify one person, organization, program, network, market, or rule on which it depends.



- » Write at least two questions that must be answered before accepting a broader claim.

Then explain why neither the word utility nor a displayed price proves that an asset is useful, liquid, safe, or legally classified in a particular way.

Important limitation of the exercise: The descriptions are simplified and hypothetical. Classification helps organize questions; it does not provide investment or legal advice and does not establish whether any asset should be created, acquired, or used.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Under this course's teaching distinction, which description best fits a coin?
 - a. Any points stored in a company's private database
 - b. A digital asset native to its own blockchain network
 - c. Every digital item created by a smart contract on another network
 - d. An asset whose price is guaranteed to remain stable
2. Which question is most useful when evaluating a token described as providing utility?
 - a. Does the advertisement repeat the word utility?
 - b. Did one recent trade show a high price?
 - c. What verified function exists, who controls it, and what restrictions or dependencies apply?
 - d. Does the token have a memorable name?
3. Which statement best describes liquidity?
 - a. A guarantee that an asset's price will rise
 - b. The ability to exchange an asset without excessive delay or a large price change
 - c. The legal classification assigned by a project's website
 - d. The number of technical terms used in a white paper

TRUE OR FALSE

- » If a token performs a real technical function, that function guarantees market value, legal compliance, and protection from fraud.



SHORT EXPLANATION

- » In three or four sentences, explain why a careful learner should examine an asset's technical identity, function, rights, control, evidence, risks, and alternatives instead of relying on the label coin, token, or utility.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Cryptocurrency is a broad label whose meaning should be defined.
- » In this course, a coin is native to its blockchain, while a token is created through code on an existing blockchain platform.
- » Industry sources do not always use coin and token consistently, so technical structure and function are more reliable than the label alone.
- » A digital asset may support fees, security, access, governance, rewards, or other functions.
- » A function does not guarantee usefulness, rights, price, liquidity, safety, or legal treatment.
- » Liquidity describes the ability to exchange an asset without excessive delay or a large price change; a displayed price does not prove liquidity.
- » Volatility, limited liquidity, fraud, technical failure, concentration, platform failure, and regulatory uncertainty are material risks.
- » A careful evaluation identifies what is known, what is claimed, who controls the system, what evidence supports the claim, and what remains unknown.

The practical skill is learning to replace a label with a structured set of questions. That habit can strengthen critical thinking even when you never own or use a digital asset.

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 the course's distinction among cryptocurrency, coin, token, and native asset.
- » Describe two non-investment functions a digital asset may perform.
- » Explain why the word utility does not prove usefulness, value, liquidity, or legal treatment.
- » Identify at least four questions you would ask before accepting a claim about a digital asset.

- » Describe one material risk and one important dependency that a promoter might leave out.
- » Use the Prison Professors Token case study to explain one fact the blockchain can help verify and one question that still depends on human accountability.
- » Explain why a conventional database, membership account, or other simpler system should sometimes be considered as an alternative.
- » Connect this evaluation process to the critical-thinking, communication, or self-directed-learning skills you are developing.

Your response should demonstrate your reasoning. You are not being asked to purchase an asset, create an account, open a wallet, connect to a network or application, disclose financial information, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 9: Cryptocurrencies, Coins, and Tokens, 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 9 — [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, or other sensitive credentials.



UNDERSTANDING WEB3**LESSON 10: STABLECOINS: USES, STRUCTURES, AND RISKS**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson provides general education about technology and risk. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any stablecoin, network, company, platform, or financial product. You do not need internet access, an account, a wallet, a stablecoin, or any other digital asset to complete the lesson.

OPENING GUIDANCE

The word stable can sound reassuring. It may suggest that an asset cannot lose value or that someone has guaranteed the result. A careful learner should not accept either assumption.

A stablecoin is a digital token designed to maintain a value relative to a reference asset, commonly a national currency such as the United States dollar. The design may work well for a period of time and then fail under stress. Different stablecoins may use very different reserves, collateral, redemption rules, computer programs, and organizations even when each one claims to equal one dollar.

I encourage you to investigate the mechanism behind the label. Ask what value the token is trying to track, what supports that target, who has a duty to redeem it, who may request redemption, what evidence is available, and what could happen if many people want their money at the same time.

This lesson will not ask you to acquire, exchange, or use a stablecoin. It will help you evaluate a promise of stability without confusing that promise with proof.

PURPOSE AND ESSENTIAL QUESTION

Lesson 10 explains why stablecoins seek price stability, describes several common support mechanisms, and examines why the word stable does not mean risk-free.

Essential Question:

- » What should a careful learner investigate before trusting a stablecoin's claim of stability?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define stablecoin and explain what a reference asset does.
- » Compare reserve-backed, crypto-collateralized, and algorithmic stability mechanisms at an introductory level.
- » Distinguish direct redemption from selling a stablecoin in a secondary market.
- » Identify reserve, issuer, custodian, redemption, liquidity, technology, depeg, and regulatory risks.
- » Evaluate a stability claim by identifying the support mechanism, available evidence, and unanswered questions.

KEY TERMS

STABLECOIN

Definition: A digital token designed to maintain a value relative to a reference asset, such as one United States dollar. The name describes an objective, not a guarantee.

Sample sentence: The learner investigated how the stablecoin attempted to maintain its one-dollar target before accepting the word stable.

REFERENCE ASSET

Definition: The currency, commodity, asset, or other measure whose value a stablecoin is designed to track.

Sample sentence: The United States dollar was the stablecoin's reference asset.

RESERVE

Definition: Assets held or managed to support a stablecoin's value and meet redemption requests.

Sample sentence: The disclosure identified cash and short-term government securities as parts of the reserve.

COLLATERAL

Definition: Assets committed to support an obligation or position and available for sale or liquidation under defined conditions.

Sample sentence: The protocol required collateral worth more than the stablecoins it created because the collateral price could fall.

REDEMPTION

Definition: The process of returning a stablecoin to an issuer or system in exchange for the referenced asset or another asset under stated rules.

Sample sentence: The learner asked who could request redemption, what fees applied, and how long the process could take.

ISSUER

Definition: The organization or system responsible for creating a digital asset and carrying out duties described in its rules or agreements.

Sample sentence: The issuer published information about the reserve and its redemption policy.

DEPEG

Definition: A movement of a stablecoin's market price away from its intended reference value.

Sample sentence: A loss of confidence caused the token to depeg and trade below its one-dollar target.

MAIN LESSON

STABILITY IS A RELATIONSHIP, NOT AN ABSOLUTE CONDITION

A stablecoin does not attempt to remain stable against everything. It tries to track a specific reference. A token targeting one United States dollar may seek to remain near one dollar. A token referencing another currency or a commodity would have a different target.

This distinction matters because a stable price in dollars does not guarantee stable purchasing power. The cost of food, housing, transportation, or other goods may still change. The term stablecoin normally describes the relationship between the token and its reference asset, not protection from inflation or every type of loss.

The term also does not have one universal technical or legal meaning. Industry participants and regulators may define stablecoin differently. For this course, we will use a practical teaching definition: a blockchain-based token designed to track



a stated reference value through reserves, collateral, program rules, market incentives, or a combination of those mechanisms.

A STABILITY CLAIM HAS SEVERAL WORKING PARTS

A careful learner can separate a stablecoin arrangement into five parts:

1. Reference: What value is the token trying to track?
2. Support mechanism: What assets, rules, or incentives are intended to keep the token near that value?
3. Issuance and redemption: How are tokens created and removed, and who may exchange them for the referenced asset?
4. Market activity: Where do other users buy or sell the token, and how does market trading affect its price?
5. People and systems: Which issuer, custodian, bank, smart contract, network, price feed, exchange, or governing group must perform correctly?

The blockchain may show token issuance, transfers, or balances. It may not show the complete reserve held in bank accounts or securities outside the blockchain. It also may not prove that a holder has an enforceable claim, that a custodian has protected the reserve, or that redemption will remain available during stress. Evidence must come from more than one place.

RESERVE-BACKED STABLECOINS DEPEND ON AN ISSUER AND OFF-CHAIN ASSETS

A reserve-backed stablecoin generally has an identifiable issuer. The issuer creates tokens and represents that assets held outside the blockchain support the tokens in circulation. Those assets may include cash, bank deposits, short-term government securities, or other financial instruments permitted by the arrangement and applicable law.

In a simplified model, an eligible customer provides one dollar to the issuer, and the issuer creates one token. When an eligible customer returns one token for redemption, the issuer removes or burns the token and returns one dollar under the issuer's rules. If users believe the issuer can perform that exchange reliably, market trading may remain close to the target.

The word backed does not answer every question. A learner should investigate:

- » What assets make up the reserve?
- » Are those assets valued frequently and held in sufficient amounts?
- » Who holds the reserve, and what happens if that custodian or bank fails?
- » Are reserve assets separated from the issuer's other assets?

- » What independent examination, attestation, or audit exists, and what exactly does it cover?
- » Does every holder have a legal right to redeem, or only certain approved customers?
- » What fees, minimum amounts, delays, freezes, or other restrictions may apply?

A reserve may appear sufficient during ordinary conditions yet become difficult to sell quickly during stress. An issuer may also face operational failure, fraud, legal restrictions, cyber incidents, or a sudden loss of confidence.

CRYPTO-COLLATERALIZED STABLECOINS DEPEND ON VOLATILE COLLATERAL AND PROGRAM RULES

Some stablecoins use crypto assets as collateral. Because crypto collateral can change value rapidly, these systems commonly require collateral worth more than the stablecoins created. This practice is called overcollateralization.

For example, a simplified system might require a user to lock collateral with a market value of \$160 before creating \$100 in stablecoins. A smart contract monitors the collateral value through a price feed. If the collateral falls below a required level, the system may sell or liquidate it to protect the stablecoin arrangement.

This design replaces some issuer functions with code and market incentives, but it does not remove dependency. The system may depend on accurate price data, smart-contract security, sufficient buyers for liquidated collateral, responsible governance, and continued demand. A rapid market decline can cause many liquidations at once. Congestion, inaccurate data, insufficient liquidity, or flawed code can make the problem worse.

ALGORITHMIC AND HYBRID DESIGNS DEPEND HEAVILY ON CONFIDENCE

An algorithmic stablecoin attempts to maintain its target through program rules and economic incentives, often by changing token supply or exchanging the stablecoin with another related token. Some versions hold little or no independent reserve. Hybrid systems combine collateral with algorithmic features.

The basic idea may sound orderly: create more tokens when the price rises above the target and reduce supply when the price falls below the target. The difficult question is whether people will continue accepting the related token, incentive, or future promise when confidence weakens.

If holders begin selling because they doubt the system, the mechanism may require still more selling, token creation, or promised future rewards. A negative cycle can accelerate rather than restore stability. Computer code can execute the rules exactly as written and the economic design can still fail.



The category algorithmic covers different designs, so a learner should not assume that every project has identical risks. The important practice is to identify the reserve, collateral, related tokens, incentives, decision makers, and failure conditions rather than relying on the category name.

REDEMPTION AND MARKET SALE ARE NOT THE SAME PROCESS

Direct redemption occurs through the issuer or protocol under stated rules. A secondary-market sale occurs when one market participant sells the token to another through an exchange or other trading venue.

Some reserve-backed issuers provide direct redemption only to approved institutions or customers who meet account, location, identity, or minimum-amount requirements. Other holders may have to sell in a secondary market. In ordinary conditions, professional traders may buy a token below the target and redeem it at the target, or create tokens at the target and sell them above it. This activity, called arbitrage, can help move the market price back toward the reference value.

That process depends on access, confidence, time, fees, and liquidity. If direct redemption is delayed or restricted, or if people doubt the reserve, sellers may accept less than the target value. A market price of \$0.98 for a token intended to equal \$1.00 is a depeg even if the issuer continues stating that direct redemption is available at one dollar.

Before trusting a redemption promise, ask who qualifies, what the holder receives, how long the process takes, what costs apply, and what conditions permit delay, suspension, or refusal.

THE WORD STABLE DOES NOT MEAN RISK-FREE

Stablecoin risk can arise from several connected parts:

- » Reserve risk: The reserve may be insufficient, difficult to value, exposed to loss, or unable to meet rapid redemptions.
- » Issuer risk: The organization may make poor decisions, fail operationally, misstate information, become insolvent, or face legal restrictions.
- » Custodian and bank risk: An institution holding reserve assets may fail, freeze access, or create delays.
- » Redemption risk: A holder may not qualify for direct redemption or may face fees, limits, delay, or suspension.
- » Liquidity and run risk: Many holders may try to exit at once, forcing reserve sales or causing the market price to fall further.



- » Collateral and liquidation risk: Volatile collateral may lose value faster than a system can sell it.
- » Technology risk: Smart contracts, price feeds, bridges, wallets, networks, or connected applications may fail or be attacked.
- » Governance risk: A small group may change parameters, approve reserve practices, pause activity, or control upgrades.
- » Regulatory and legal risk: Rules, rights, and permitted uses may vary by jurisdiction and change over time.
- » Fraud and impersonation risk: A fake token may copy the name or symbol of a legitimate project, and dishonest promoters may invent reserve claims.

A stablecoin can remain near its target and still expose a user to theft, frozen access, platform failure, privacy concerns, or legal restrictions. Price stability addresses only one part of risk.

A STABLECOIN IS NOT AUTOMATICALLY AN INSURED BANK DEPOSIT

The fact that a token references the United States dollar does not make the token a bank account. In the United States, the Federal Deposit Insurance Corporation states that crypto assets are not FDIC-insured deposits. A bank deposit used somewhere in an issuer's reserve does not automatically give each token holder deposit-insurance protection.

As of July 21, 2026, United States agencies were implementing a new federal framework for payment stablecoins. An April 2026 FDIC proposal stated that deposits held as reserves for a permitted payment stablecoin issuer would not receive pass-through deposit insurance for stablecoin holders. The rules remain time-sensitive and do not settle the treatment of every stablecoin, holder, transaction, or jurisdiction.

This lesson does not provide a legal conclusion. It teaches a durable question: what exact legal claim and protection does the holder have, and which official source supports that answer?

STABLECOINS MAY SUPPORT USEFUL ACTIVITY WITHOUT ELIMINATING TRADEOFFS

Stablecoins may be used as a settlement asset within digital-asset markets, a unit for quoting prices, a component in decentralized applications, or a way to transfer value across networks and borders. A person or business may value faster availability, programmability, or the ability to use a blockchain-based application.

Those possible benefits depend on the complete system. A transfer may still involve network fees, wallet security, platform access, identity requirements, exchange rates,



taxes, sanctions rules, scams, and the risk of sending to a wrong address or network. A conventional bank transfer, money order, or other payment method may provide stronger protections or be more appropriate for a particular situation.

This course does not ask participants to choose a payment method. It asks them to compare function, cost, access, protection, responsibility, and risk.

RETURNING BRIEFLY TO THE PRISON PROFESSORS CASE: WBNB IS NOT A STABLECOIN

Lesson 9 introduced WBNB, or Wrapped BNB, when discussing the public treasury associated with the independent Prison Professors Token community. WBNB is a token representation of BNB that can interact with applications using a token standard.

Wrapping changes the technical form; its primary purpose is compatibility, not reducing price volatility or keeping the asset worth one United States dollar. WBNB generally follows the value of BNB. If BNB's dollar price changes, WBNB's dollar price generally changes with it. The case helps us separate two ideas that may sound similar: a wrapped token is designed to represent another crypto asset, while a stablecoin is designed to maintain a relatively stable value against its stated reference.

A DISCIPLINED STABLECOIN EVALUATION

Before accepting a stablecoin claim, organize the investigation around these questions:

1. Reference: What value is the token designed to track?
2. Mechanism: Does it use off-chain reserves, crypto collateral, algorithms, or a combination?
3. Evidence: What current, independent information supports the reserve or collateral claim?
4. Redemption: Who may redeem directly, for what asset, at what rate, with what cost and delay?
5. Control: Who issues tokens, holds assets, changes rules, supplies price data, pauses activity, or governs upgrades?
6. Stress: What happens if collateral falls, a custodian fails, markets become illiquid, or many holders seek redemption at once?
7. Rights and protection: What legal claim does a holder have, and what laws, insurance, or remedies actually apply?
8. Alternatives: Could a bank deposit, ordinary payment service, or other system meet the need with different protections and risks?

A clear answer should identify both evidence and uncertainty. If a person cannot explain the support mechanism and redemption path, the word stable provides too little information for a reasoned conclusion.

APPLIED SCENARIO: THREE CLAIMS OF STABILITY

A program provides three hypothetical descriptions. None of the tokens is real.

RESERVEDOLLAR

ReserveDollar targets one United States dollar. A company issues the token and says the reserve contains cash and short-term government securities. It publishes a monthly total but does not identify the custodian or provide an independent examination. Direct redemption is available only to approved business customers with a \$100,000 minimum. Other holders must sell through a market.

COLLATERALDOLLAR

CollateralDollar targets one United States dollar. Users lock crypto assets worth at least 160 percent of the stablecoins they create. Smart contracts use an outside price feed and may liquidate collateral if its value falls. The description does not explain what happens if the price feed fails or many positions require liquidation at the same time.

BALANCEDOLLAR

BalanceDollar targets one United States dollar but holds no separate reserve. A program creates or destroys BalanceDollar and a related token to influence supply. Its website says community confidence will keep the system stable. It does not explain what supports the related token if demand for both assets falls.

Reasoned comparison: Each token states the same target, but the support mechanisms and risks differ. ReserveDollar depends on the issuer, reserve quality, custodian, evidence, and limited redemption path. CollateralDollar depends on volatile collateral, reliable code, accurate price data, and orderly liquidation. BalanceDollar depends heavily on continuing demand and confidence in a related token. A careful learner would not rank the tokens by name. The learner would identify the mechanism, evidence, redemption rights, control points, and stress conditions before reaching a conclusion.



BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » A stable reference may make some blockchain transactions and records easier to understand.
- » A stablecoin may support settlement, transfer, pricing, or application functions without requiring every step to use a volatile native asset.
- » Programmable tokens can interact with smart contracts and other compatible applications.
- » Public blockchain records may show issuance, transfers, and token balances.

IMPORTANT LIMITATIONS AND RISKS

- » A target price does not guarantee that the market price or redemption value will remain at the target.
- » Reserves, collateral, issuers, custodians, smart contracts, price feeds, and markets can fail.
- » Public token records do not by themselves prove the quality, location, or legal protection of off-chain reserves.
- » Direct redemption may be unavailable to many holders.
- » A stablecoin may depeg, become illiquid, be frozen, or lose all or part of its value.
- » Legal treatment and user protections vary and may change.

COMMON MISCONCEPTIONS

- » “Stablecoin means guaranteed.” Stable describes a design objective, not a promise that cannot fail.
- » “One token equals one dollar because the website says so.” A claim requires evidence about support and redemption.
- » “Backed means every holder owns part of the reserve.” Legal rights depend on the arrangement and applicable law.
- » “A reserve report proves everything.” The scope, timing, valuation, independence, and limitations of the report matter.
- » “If a token trades near one dollar today, it cannot depeg tomorrow.” Market confidence and conditions can change quickly.
- » “A stablecoin is the same as an insured bank account.” A crypto token and an insured deposit are different legal and operational arrangements.



- » “WBNB is a stablecoin because it is designed to track BNB.” WBNB represents BNB and generally changes in dollar value with BNB; it does not target one dollar.

OFFLINE EXERCISE: INVESTIGATE THE MECHANISM

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Review ReserveDollar, CollateralDollar, and BalanceDollar from the applied scenario. For each description, create six headings:

1. Reference value
2. Support mechanism
3. Redemption path
4. Control and dependencies
5. Evidence provided
6. Missing information and stress risks

Under each heading, write what the description establishes and what remains unknown. Then answer these questions:

- » Which description provides the clearest redemption path, and what important restriction remains?
- » Which description depends most directly on volatile crypto collateral and liquidation?
- » Which description depends most heavily on continuing market confidence without a separate reserve?
- » What additional evidence would you request for each description?
- » Why would the shared label stablecoin be an inadequate basis for deciding that the three arrangements have equal risk?

Conclude with four or five sentences explaining which questions from the disciplined evaluation framework were most useful and why.

Important limitation of the exercise: These descriptions are simplified and hypothetical. The exercise develops reasoning; it does not recommend a stablecoin, rank a real product, or provide financial or legal advice.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. What does the word stablecoin most accurately describe in this lesson?
 - a. A token whose value cannot change
 - b. A token designed to track a stated reference value
 - c. An insured bank account recorded on a blockchain
 - d. Any wrapped version of a native asset
2. Which question is most useful when evaluating a reserve-backed stablecoin?
 - a. Does the token use the word dollar in its name?
 - b. Does a promoter say that everyone trusts it?
 - c. What assets support it, who holds them, who may redeem, and what evidence verifies the claim?
 - d. Has its symbol appeared frequently on social media?
3. Which statement best distinguishes direct redemption from a secondary-market sale?
 - a. Direct redemption follows the issuer's or protocol's rules, while a market sale depends on another buyer and market conditions.
 - b. Direct redemption and market sale always provide the same price and timing.
 - c. Only a secondary-market sale can remove tokens from circulation.
 - d. Direct redemption is available automatically to every person in every jurisdiction.

TRUE OR FALSE

- » If a stablecoin has remained close to one dollar for a long period, it has no reserve, redemption, technology, liquidity, or legal risk.

SHORT EXPLANATION

- » In three or four sentences, explain why two stablecoins with the same one-dollar target may have different risks.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A stablecoin is a token designed to track a reference value; the name does not guarantee success.



- » Stability is relative to a stated reference and does not protect against every kind of loss or changing purchasing power.
- » Reserve-backed, crypto-collateralized, algorithmic, and hybrid designs rely on different mechanisms and dependencies.
- » Direct redemption differs from selling through a secondary market.
- » Reserve quality, custody, redemption rights, market liquidity, technology, governance, and legal protections all matter.
- » A public blockchain record may show token activity without proving the condition or legal protection of off-chain reserves.
- » A stablecoin may depeg when confidence, liquidity, collateral, redemption, or operations fail.
- » A stablecoin is not automatically an FDIC-insured bank deposit.
- » WBNB is a wrapped representation of BNB, not a stablecoin targeting one dollar.

The practical skill is learning to ask what supports the stability claim and what happens under stress. That reasoning can help you evaluate many systems in which a confident label hides important dependencies.

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 stablecoin in your own words and explain why stable does not mean risk-free.
- » Compare reserve-backed, crypto-collateralized, and algorithmic support mechanisms.
- » Explain the difference between direct redemption and a secondary-market sale.
- » Choose one token from the Three Claims of Stability scenario and identify its reference, support mechanism, dependencies, evidence, and missing information.
- » Describe one condition that could cause the token to depeg.
- » Explain why a stablecoin should not automatically be treated as an insured bank deposit.
- » Connect the evaluation process to the critical-thinking, research, communication, or self-directed-learning skills you are building.



Your response should demonstrate your reasoning. You are not being asked to purchase a stablecoin, open an account, create a wallet, connect to a network or application, disclose financial information, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 10: Stablecoins: Uses, Structures, and Risks, 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 10 — [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, or other sensitive credentials.

UNDERSTANDING WEB3**LESSON 11: TOKENIZATION AND NON-FUNGIBLE TOKENS**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

This lesson provides general education about technology, records, rights, and risk. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend any token, network, company, marketplace, platform, or financial product. You do not need internet access, an account, a wallet, an NFT, or any other digital asset to complete the lesson.

OPENING GUIDANCE

A token can carry a confident label: certificate, ticket, membership, artwork, title, or ownership. The label may describe an intended relationship, but it does not prove that the relationship is valid.

I encourage you to separate the digital record from the claim attached to it. Ask who created the token, what the token points to, what rights the issuer promised, what evidence supports the promise, where important information is stored, and whether another person or institution recognizes the result.

That habit is useful far beyond Web3. A document, badge, database entry, or certificate has value because people can verify who issued it, what it means, and whether the issuer had authority. Technology can strengthen part of that process. It cannot make an unsupported claim true.

This lesson will not ask you to create, purchase, transfer, or display a token. It will help you evaluate what a token record can establish and what still depends on off-chain evidence, legal rights, storage, and human judgment.

PURPOSE AND ESSENTIAL QUESTION

Lesson 11 explains how tokens can represent access, records, rights, or unique items while separating the blockchain token from the underlying legal or practical claim.

Essential Question:

- » What does a token record actually prove, and what must be verified somewhere else?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define tokenization, fungible, and non-fungible token.
- » Distinguish a token record from the item, file, service, credential, or legal right it may reference.
- » Identify possible uses in credentials, tickets, property records, creative work, and membership.
- » Explain how metadata and storage choices affect a tokenized system.
- » Evaluate ownership, copyright, authenticity, privacy, fraud, and legal limitations while comparing tokenization with an ordinary database.

KEY TERMS

TOKENIZATION

Definition: The process of using a digital token to represent an item, record, right, claim, or form of access. The token and the thing it represents are related but not automatically identical.

Sample sentence: The organization considered tokenization for course certificates but first examined whether a conventional credential database would meet the same need.

FUNGIBLE

Definition: Interchangeable with another unit of the same type and value.

Sample sentence: One unit of a fungible token is designed to be equivalent to another unit of the same token.

NON-FUNGIBLE TOKEN

Definition: A distinguishable blockchain token identified separately from other tokens, commonly by a smart-contract address and a token identification number. An NFT can reference an item or claim without containing or legally controlling that item or claim.

Sample sentence: The non-fungible token had its own identification number, but the learner still investigated what rights came with it.

METADATA

Definition: Information that describes other data, such as a token's name, description, image location, certificate details, or attributes.

Sample sentence: The metadata listed the course title and completion date and pointed to an external certificate file.

OWNERSHIP

Definition: A relationship of control or legal rights over property, a record, or an asset. Control of a token does not automatically establish ownership of everything the token references.

Sample sentence: The agreement explained whether token ownership included access, a license, or only control of the token itself.

AUTHENTICITY

Definition: The quality of being genuine and connected to the claimed source.

Sample sentence: The verifier checked the issuer's identity and authority before accepting the tokenized certificate as authentic.

MAIN LESSON

TOKENIZATION CREATES A REPRESENTATION

Tokenization connects a digital token with something else. That something might be access to an event, membership in a community, a course credential, a record about a physical item, a creative work, or a financial or legal interest.

The word represent is important. A paper ticket represents permission to enter an event, but the piece of paper does not create the event. A vehicle title represents a legally recognized relationship with a vehicle, but the title is not the vehicle. A course certificate represents an issuer's statement that a person met stated requirements, but the certificate is not the learning itself.

A blockchain token works in a similar way. The blockchain can record that a particular token was created, assigned, or transferred under the rules of a smart contract. Whether the token delivers a valid ticket, credential, license, property right, or membership benefit depends on more than the blockchain entry.

Tokenization can organize a relationship. It cannot supply missing authority, evidence, or legal recognition.

FUNGIBLE AND NON-FUNGIBLE DESCRIBE HOW UNITS ARE TREATED

Fungible units are designed to be interchangeable. If two people exchange equal units of the same fungible token, neither person is supposed to receive a uniquely distinguished unit.

Non-fungible tokens are tracked separately. A common NFT standard assigns each token a distinct identification number within a smart contract. The complete identifier depends on more than the number alone. A careful description includes the blockchain network, the smart-contract address, and the token ID. Two unrelated contracts can both issue a token numbered 100.

Non-fungible does not mean that the associated picture, file, or idea cannot be copied. It means the token record is distinguishable. A unique token can still be meaningless, fraudulent, technically broken, or disconnected from a real benefit.

AN NFT HAS SEVERAL CONNECTED LAYERS

A beginner can understand an NFT by separating five layers:

1. Network and smart contract: The blockchain and code that create and manage the token.
2. Token record: The token ID, current blockchain address, and transfer history recorded under the contract's rules.
3. Metadata: Information describing the token and often pointing to a file or external record.
4. Referenced item or service: The image, ticket, certificate, physical object, membership, or other subject connected to the token.
5. Rights and recognition: The agreement, policy, law, issuer, institution, or community that gives the token practical or legal meaning.

These layers may work together, but they can also separate. The token can continue to exist after an event is canceled. The metadata can point to a file that is later removed. The physical item can be damaged. The issuer can stop honoring a membership benefit. A license can limit how a creative work may be used. A government record can remain the legally controlling record even if a separate token claims to represent the same property.

The strongest analysis follows the complete chain from code to real-world recognition.

WHAT THE BLOCKCHAIN RECORD MAY ESTABLISH

Under the rules of a functioning network and smart contract, a public blockchain record may help a verifier determine:

- » Which smart contract created or manages the token.
- » Which token ID is being examined.
- » Which blockchain address currently controls the token according to the contract.
- » When the token was created or transferred on that network.
- » Whether the contract permits transfers, approvals, destruction, pausing, or updates.
- » Which metadata location or other data the contract currently returns.

Those facts create a shared history that different participants may inspect.

Even these conclusions require care. A blockchain address does not identify a human being by itself. A transfer record shows what the network accepted; it does not automatically show whether the transfer was voluntary, authorized under an outside agreement, or recognized by law.

WHAT THE BLOCKCHAIN RECORD CANNOT PROVE BY ITSELF

A token record does not automatically prove:

- » That the person who created the token owned or had authority over the referenced item.
- » That an image or file is original rather than copied.
- » That the physical item exists, remains in good condition, or matches its description.
- » That the holder received copyright, trademark, property title, or another legal right.
- » That a ticket issuer will admit the holder to an event.
- » That a school, employer, licensing body, court, or government agency recognizes a credential or record.
- » That the person presenting the token controls the identity named in the metadata.
- » That off-chain information will remain available, accurate, private, or unchanged.

This boundary is central to the lesson. A blockchain can preserve evidence about a token. It cannot independently verify every fact outside the blockchain.



METADATA CAN CONNECT THE TOKEN TO INFORMATION STORED ELSEWHERE

NFT standards commonly allow a token to provide a location for metadata. The metadata may contain a name, description, image link, certificate information, or other attributes. It may be stored directly on a blockchain, on a decentralized storage system, or on an ordinary web server.

Storing a large file directly on a blockchain can be expensive and may create privacy or permanence problems. For that reason, many NFT-associated files are stored somewhere else. The blockchain token then points to the location.

THIS DESIGN CREATES DEPENDENCIES:

- » A web server can stop operating or change the file.
- » A link can break.
- » A decentralized storage reference may remain valid while the content is no longer readily available.
- » Metadata may be updateable by an administrator, which can be useful for corrections but can also change what the token appears to represent.
- » Permanent public storage may conflict with privacy, correction, or deletion needs.

Examine the phrase stored on the blockchain precisely. Is the entire file on-chain, or only a token ID and link? Is the metadata fixed or changeable? Who controls updates? What happens if the external location disappears?

TOKEN CONTROL, POSSESSION, CONTRACT RIGHTS, AND COPYRIGHT ARE DIFFERENT

The word ownership can hide several separate relationships. Token control concerns the functions a blockchain address may exercise. Possession concerns control of the referenced copy or object. Contract rights come from stated terms, such as event admission or membership access. Copyright includes legal rights related to an original creative work. Owning a copy of a painting does not normally mean owning the copyright in the painting. The same separation applies to an NFT and an associated work.

A March 2024 report from the United States Copyright Office and United States Patent and Trademark Office explained that transferring an NFT transfers the digital token but does not necessarily transfer the associated asset or copyright rights. A separate agreement is ordinarily needed to transfer copyright or other associated rights. That United States report is dated legal context, not advice about a particular token or transaction.

The practical lesson is durable: read the actual terms. Ask whether the token provides access, a personal-use license, commercial rights, a claim against an issuer,



possession of an object, or only control of the token. Do not let the word owner replace that investigation.

AUTHENTICITY DEPENDS ON THE ISSUER AND THE EVIDENCE

A blockchain can make a record difficult to alter without detection, yet still preserve false information. If an unauthorized person creates a token that points to someone else's artwork, the blockchain can accurately record the unauthorized token.

Authenticity therefore begins with the source. Who is the issuer? How can a verifier connect the issuer's real identity with the issuing smart contract or address? Did the issuer have authority over the referenced item? What process did the issuer follow before creating the token? Is there an outside record, signed statement, institutional policy, or recognized registry that supports the claim?

The same reasoning applies to a tokenized certificate. A verifier must know whether the named institution issued it, whether the recipient completed the work, whether the credential remains valid, and whether the token is linked responsibly to the correct person.

CREDENTIALS DO NOT REQUIRE NFTS OR BLOCKCHAINS

Digital credentials can be designed in many ways. The World Wide Web Consortium's Verifiable Credentials standard describes an issuer, a holder, and a verifier. It includes ways to secure claims against tampering without requiring every credential to be an NFT or a public blockchain record.

The goal should guide the technology. A signed digital certificate, controlled database, standards-based verifiable credential, or blockchain token might address parts of a school's need. The best design depends on access, privacy, correction, revocation, cost, interoperability, governance, and trust.

POSSIBLE USES REQUIRE DIFFERENT KINDS OF RECOGNITION

Tokenization may be proposed for several purposes:

- » Tickets: A token may identify an admission credential, but the organizer must recognize it and address mistakes or lost access.
- » Membership: A token may unlock services, but the organization must define benefits, duration, transfer, and recovery.
- » Credentials: A token may reference an achievement, but issuer identity, assessment, privacy, and revocation still matter.
- » Creative work: An NFT may reference art, music, or writing, while creator authorization, storage, license terms, and copyright remain separate.

- » Physical property or records: A token may track an object or proposed interest, but a registry, contract, institution, or law may control the recognized right.

In the United States, legal treatment depends on facts and circumstances. A January 2026 statement from three divisions of the Securities and Exchange Commission explained that tokenized securities can use different structures and provide different rights. A third-party token may not provide the same rights as the underlying security and may add counterparty risk. The broader lesson applies beyond securities: tokenization does not change the underlying claim by magic.

BNB SMART CHAIN CAN HOST TOKENS, BUT THE NETWORK DOES NOT VALIDATE EVERY CLAIM

BNB Smart Chain is compatible with the Ethereum Virtual Machine and related smart-contract tooling. Developers can therefore deploy token contracts using interfaces similar to widely used Ethereum standards.

This technical compatibility explains how an NFT can exist on BNB Smart Chain. It does not show that a particular NFT is authentic, valuable, authorized, or legally effective. The network can process the smart contract and record transfers while the associated claim remains false, incomplete, or dependent on an outside agreement.

The recurring BNB Chain example reinforces a distinction used throughout this course: a platform can provide technical capability without endorsing every project built on it.

WHEN AN ORDINARY DATABASE MAY WORK BETTER

A blockchain may add value when independent participants need a shared history, public verification is appropriate, and the benefits outweigh cost, privacy, governance, and error risks.

An ordinary database may work better when one organization already has clear authority, records require correction or deletion, personal information should remain private, users need reliable recovery, activity is high-volume and inexpensive, or outside institutions recognize only the organization's official records.

For an event organizer that controls issuance, admission, refunds, and customer service, a centralized ticket database may provide simpler correction and recovery. A token may add portability or programmable rules while also introducing wallet access, fees, scams, privacy concerns, and irreversible errors. Compare complete systems and ask which approach solves the problem with acceptable cost, access, accountability, and risk.

A DISCIPLINED TOKENIZATION EVALUATION

Before accepting a tokenization claim, ask:

PRISON PROFESSORS CHARITABLE CORPORATION



1. Subject: What item, service, record, right, or claim does the token supposedly represent?
2. Issuer: Who created the token, and how can that identity and authority be verified?
3. Token record: What does the blockchain show about the contract, token ID, address, transfers, and control functions?
4. Metadata and storage: What information or file does the token reference, where is it stored, can it change, and who keeps it available?
5. Rights: What access, license, ownership interest, benefit, or remedy is actually promised in the governing terms?
6. Recognition: Which person, institution, registry, marketplace, or legal system recognizes the claim?
7. Failure conditions: What happens if access credentials are lost, metadata disappears, the issuer fails, the contract contains an error, or the token was created without authority?
8. Alternative: Could an ordinary database, signed document, conventional ticket, or other credential solve the problem more safely or simply?

A careful answer separates established facts from unresolved claims. The token may be one useful piece of evidence. It should not be treated as the complete proof without investigating the rest of the system.

APPLIED SCENARIO: THE TOKENIZED COURSE CERTIFICATE

The following organization and certificate are hypothetical.

LearningBridge Institute offers a 12-week job-readiness course. After a participant completes the reading, written assignments, and final project, the institute creates a non-transferable NFT called LearningBridge Completion Certificate #1842 on a public blockchain.

The token record shows the issuing smart contract, token ID 1842, the date of creation, and the blockchain address that received it. The metadata lists the course title, completion date, and a link to a certificate file stored on the institute's web server. The institute's website says employers can trust every token issued by the contract.

The description leaves important questions unanswered:

- » How does an employer verify that the smart contract belongs to LearningBridge Institute?



- » What evidence shows that the institute is a legitimate organization and that it followed the stated assessment process?
- » How is the blockchain address connected to the correct participant without exposing sensitive personal information?
- » Can the metadata or certificate file be changed?
- » What happens if the web server stops operating?
- » Can the institute correct a misspelled name or revoke a certificate issued by mistake?
- » Does non-transferable mean the credential cannot be shared, stolen through lost account access, or displayed by the wrong person?
- » Will employers recognize the credential, and what process will they use to verify it?
- » Could a signed digital certificate and an ordinary verification database meet the same need with easier recovery and privacy?

Reasoned conclusion: The blockchain record can help show that token 1842 was created by a particular contract and assigned to a particular address. It cannot independently prove the institute's legitimacy, the participant's identity, completion of the course, employer acceptance, or continued availability of the linked certificate. A strong credential system must connect the token record with verified issuer identity, a trustworthy assessment process, durable storage, privacy protections, correction and revocation rules, and a practical verification method.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » A shared token record may make issuance and transfer history easier for different participants to inspect.
- » Standard token interfaces may allow compatible wallets and applications to recognize the same type of token.
- » Programmable rules may control transferability, access, expiration, or other defined functions.
- » A token may support portable membership, ticketing, credential, or record-keeping experiments.
- » A public history may help establish when a token was created or moved under the network's rules.

IMPORTANT LIMITATIONS AND RISKS

- » The issuer may lack authority or make a false claim.
- » The associated file, benefit, physical item, or service may disappear or differ from its description.
- » Metadata may change, links may fail, and outside storage may become unavailable.
- » Smart-contract errors, stolen credentials, misleading interfaces, or network problems may cause loss or confusion.
- » Public records may create privacy risks by connecting activity, identities, memberships, or credentials.
- » Token control may not include copyright, title, possession, admission, or other legal rights.
- » A copied name, image, symbol, or website can make a fraudulent token look legitimate.
- » A specialized token system may add cost and complexity when a database or signed document would work better.
- » Legal treatment varies by jurisdiction, claim, agreement, and facts and may change over time.

COMMON MISCONCEPTIONS

- » “Non-fungible means the image cannot be copied.” The token is distinguishable; an associated file may still be viewed or copied.
- » “If it is on a blockchain, it must be authentic.” A blockchain can preserve a record of an unauthorized or false token.
- » “The token contains the artwork or certificate.” Many tokens contain an identifier and metadata that point to a file stored elsewhere.
- » “Owning the NFT means owning the copyright.” Copyright and token control are separate unless valid terms transfer or license rights.
- » “A transfer on the blockchain transfers every real-world right.” An outside agreement, registry, law, or institution may control the recognized right.
- » “A non-transferable token proves the presenter’s identity.” A token can be restricted from transfer while the connection between an address and a person remains unverified.
- » “Tokenization is always more advanced than a database.” A simpler system may provide better privacy, recovery, correction, cost, and accountability.

OFFLINE EXERCISE: WHAT CAN THE CERTIFICATE PROVE?

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Review the LearningBridge Completion Certificate scenario. Create two headings on separate paper:

1. Supported by the token record
2. Requires outside evidence or recognition

Place each statement below under the better heading. If a statement depends on both, explain the boundary.

- » Token ID 1842 exists under a particular smart contract.
- » A particular blockchain address received the token on the recorded date.
- » LearningBridge Institute controls the issuing contract.
- » The participant completed the required course work.
- » The participant named in the certificate controls the receiving address.
- » The certificate file remains available at the metadata link.
- » An employer recognizes the credential.
- » The institute can correct or revoke a mistaken credential.
- » The token has not been transferred under the contract's recorded history.
- » The institute had authority to make every statement in the metadata.

THEN ANSWER THESE QUESTIONS:

- » What additional evidence would help connect the smart contract to the institute?
- » What process could protect the participant's privacy while allowing verification?
- » Which correction, revocation, recovery, and storage rules are missing?
- » What could a conventional credential database establish more easily?
- » Under what conditions might the token add practical value?

Conclude with four or five sentences explaining why the token record should be treated as one part of a credential system rather than the entire proof.

Important limitation of the exercise: The organization, contract, certificate, and token are fictional. The exercise develops reasoning and does not recommend creating or using an NFT.



KNOWLEDGE CHECK

MULTIPLE CHOICE

1. What does tokenization mean in this lesson?
 - a. Turning every physical object into cryptocurrency
 - b. Using a digital token to represent an item, record, right, claim, or form of access
 - c. Proving that every tokenized claim is legally enforceable
 - d. Storing every associated file directly on a blockchain
2. Which statement best describes a non-fungible token?
 - a. It is guaranteed to be valuable because it is unique.
 - b. It cannot reference a file stored outside the blockchain.
 - c. It is tracked as a distinguishable token, commonly by a contract and token ID.
 - d. It automatically transfers copyright in any associated creative work.
3. Which question is most important when evaluating a tokenized certificate?
 - a. Does the token have an attractive image?
 - b. Did the issuer use a public blockchain?
 - c. Who issued the credential, what does the record prove, and what outside evidence supports the claim?
 - d. Can the token be discussed on social media?

TRUE OR FALSE

- » A blockchain record showing that an address controls an NFT automatically proves that the person controlling the address owns every legal right connected to the referenced item.

SHORT EXPLANATION

- » In three or four sentences, explain why a tokenized record and the item or right it represents should be evaluated separately.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Tokenization uses a digital token to represent an item, record, right, claim, or form of access.
- » Fungible units are interchangeable; non-fungible tokens are tracked separately.
- » An NFT's full identity depends on its network, smart contract, and token ID.



- » The token record, metadata, referenced item, and governing rights are connected but distinct.
- » A blockchain may show creation, address control, and transfer history without proving outside facts.
- » Metadata and associated files may be stored off-chain and may change or become unavailable.
- » Token control does not automatically include possession, copyright, title, admission, or institutional recognition.
- » Authenticity depends on a verified issuer, authority, evidence, and a reliable connection between the token and the claim.
- » Public credentials and membership records can create privacy, correction, revocation, and recovery challenges.
- » BNB Smart Chain can host token contracts, but the network does not validate every project's claim.
- » An ordinary database, signed document, or standards-based credential may solve some problems more simply.

The practical skill is learning to ask what each layer proves. A token can strengthen a record without becoming the item, right, or truth that the record describes.

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 tokenization and non-fungible token in your own words.
- » Explain the difference between a token record and the item, service, file, credential, or right it may reference.
- » Use the LearningBridge scenario to identify two facts supported by the blockchain record and two claims requiring outside evidence.
- » Explain why token control does not automatically transfer copyright or another legal right.
- » Identify one possible benefit and two risks or limitations of a tokenized credential.
- » Compare the tokenized certificate with an ordinary database or signed digital certificate.
- » State when tokenization might add value and when a simpler system might be more responsible.

- » Connect this evaluation to the critical-thinking, research, communication, or self-directed-learning skills you are building.

Your response should demonstrate your reasoning. You are not being asked to create a token, open an account, use a wallet, connect to a network or marketplace, disclose personal or financial information, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 11: Tokenization and Non-Fungible Tokens, 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 11 — [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, or other sensitive credentials.

UNDERSTANDING WEB3

SECTION 3 REVIEW: DIGITAL ASSETS AND TOKENIZATION

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. It does not recommend any network, company, product, token, or digital asset. You do not need internet access, an account, a wallet, or a digital asset to complete this review.

REVIEW PURPOSE

You have completed Lessons 9 through 11 of Understanding Web3. This review gives you a place to pause, strengthen your vocabulary, and connect the ideas of digital assets, stablecoins, tokenization, and non-fungible tokens before moving into the next section.

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, study the relevant passage, and revise your response. That cycle can help you develop the habits of a self-directed learner.

THE REVIEW COVERS:

- » The distinction among a blockchain network, its native asset, and tokens created through code on that network.
- » How function, rights, control, liquidity, and risk should be evaluated instead of inferred from labels such as coin, utility, or stable.
- » How different stablecoin structures depend on reserves, collateral, issuers, program rules, redemption, markets, and confidence.
- » How tokenization and non-fungible tokens connect a blockchain record with metadata, an issuer, a referenced item or service, and rights that may depend on outside evidence.

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 compare alternatives.
- » 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 complete.

PART 1: KNOWLEDGE QUESTIONS

MULTIPLE CHOICE

1. Under this course's teaching distinction, which statement best describes a token?
 - a. A digital asset created and recorded through code on an existing block-chain platform
 - b. The native asset built into every blockchain's base protocol
 - c. Any points recorded in a conventional company database
 - d. A digital asset whose usefulness and price are guaranteed
2. Which statement correctly classifies the principal digital assets in the Prison Professors community case study?
 - a. PP is the native asset of BNB Smart Chain, and BNB is a token created by the PP contract.
 - b. BNB is the native asset of BNB Smart Chain, while PP and WBNB are tokens that use the network.
 - c. BNB, PP, and WBNB are three names for the same asset.
 - d. WBNB is a stablecoin designed to maintain a value of one United States dollar.
3. Which statement best describes liquidity?
 - a. A guarantee that an asset will keep or increase its market value
 - b. The ability to exchange an asset without excessive delay or a large change in price



- c. The legal ownership rights attached to every token
 - d. The amount of information stored in a token's metadata
4. Which question is most useful when evaluating a stablecoin described as reserve-backed?
 - a. Does its name include the word dollar?
 - b. Does one market screen show a price near the target value?
 - c. What assets support it, who holds them, what evidence is available, and who can redeem under what rules?
 - d. Does an advertisement call it safer than every alternative?
 5. Which statement accurately distinguishes redemption from a market sale?
 - a. Redemption follows the issuer's or system's stated exchange process, while a market sale depends on finding a buyer and available liquidity.
 - b. Redemption and a market sale always produce the same result at the same price.
 - c. Redemption is possible for every holder of every stablecoin without fees, delay, or limits.
 - d. A market sale proves that the reserve contains the assets an issuer describes.
 6. Which statement best describes the relationship between an NFT and an item or file it references?
 - a. The token, referenced item, metadata, and legal rights are automatically the same thing.
 - b. The NFT must contain the entire referenced file directly on the blockchain.
 - c. The blockchain can record a distinguishable token, while metadata, storage, the referenced item, and governing rights may exist in separate layers.
 - d. The NFT guarantees that the issuer had authority to create it.
 7. Which question is most important when evaluating a tokenized certificate?
 - a. Is the token image attractive?
 - b. Who issued it, what does the blockchain record establish, what outside evidence supports the claim, and who recognizes it?
 - c. Can the certificate be discussed on social media?
 - d. Does the token have a displayed market price?



TRUE OR FALSE

- » If a token has a real utility, that function guarantees market value, liquidity, legal compliance, and protection from fraud.
- » A stablecoin may move away from its intended reference value when confidence, reserves, collateral, redemption, markets, or program rules fail to operate as expected.

SHORT EXPLANATION

- » A promoter states, “Our token is stable because it is on a blockchain, and its tokenized certificate is automatically authentic and legally binding.” In four to six sentences, explain why a careful learner should separate the token record from the stability mechanism, issuer authority, metadata and storage, referenced certificate, and governing rights. Identify at least two types of evidence or process needed to evaluate the claim.

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. Native asset
- b. Token
- c. Utility
- d. Liquidity
- e. Stablecoin
- f. Reserve
- g. Redemption
- h. Depeg
- i. Tokenization
- j. Non-fungible token
- k. Metadata
- l. Authenticity

DEFINITIONS

1. Information that describes other data, such as a token’s name, attributes, certificate details, or file location.



2. The ability to buy, sell, or exchange an asset without excessive delay or a large change in price.
3. The quality of being genuine and connected to the claimed source.
4. A digital asset built into a blockchain protocol and commonly used for functions such as paying network fees or supporting network security.
5. A digital token designed to maintain a value relative to a reference asset; the objective is not a guarantee.
6. The process of returning a stablecoin to an issuer or system in exchange for the referenced asset or another asset under stated rules.
7. A digital asset created and recorded through code on an existing blockchain platform rather than serving as that platform's native asset.
8. The process of using a digital token to represent an item, record, right, claim, or form of access.
9. A practical function or use that an asset is designed to support within a network, application, or service.
10. Assets held or managed to support a stablecoin's value and meet redemption requests.
11. A distinguishable blockchain token identified separately from other tokens, commonly by a smart-contract address and token identification number.
12. A movement of a stablecoin's market price away from its intended reference value.

PART 3: APPLIED SCENARIO — THE PATHWAY LEARNING SYSTEM

A group of education providers proposes a digital system for course payments, learner access, and completion records. The proposal contains three related components:

- » Pathway Chain is described as the base blockchain network. Its native asset, PathCoin, is used for network transaction fees.
- » StudyDollar is a fungible token created through a smart contract on Pathway Chain. The issuer says that one StudyDollar is designed to track one United States dollar. Its website says the reserve contains cash and short-term investments, but it provides no independent report, does not identify where the assets are held, and does not explain whether learners can redeem directly. Learners may be able to sell the token through a separate marketplace if buyers are available.
- » CompletionPass #742 is a non-fungible token created by a contract that uses the name FutureSkills Institute. Its metadata lists a learner's name and



completion date and points to a certificate file stored on the institute's website. The proposal does not explain how the contract was connected to the institute, how the learner was connected to the receiving address, whether the metadata can change, what happens if the website closes, or whether an employer recognizes the certificate.

The promotional materials state: "Every StudyDollar is permanently worth one dollar because it is on a blockchain. CompletionPass proves the learner's identity, course completion, legal ownership, and copyright. Blockchain records are permanent, so no outside verification, storage plan, redemption process, or conventional database is necessary."

SCENARIO QUESTIONS

1. Classify PathCoin, StudyDollar, and CompletionPass #742. Identify which is the native asset, which is a fungible token described as a stablecoin, and which is a non-fungible token.
2. Identify StudyDollar's reference asset, claimed reserve, issuer role, and missing redemption information. What evidence would you request before accepting the stability claim?
3. Explain the difference between redeeming StudyDollar and selling it in a marketplace. How could limited liquidity or loss of confidence contribute to a depeg?
4. List at least two facts the blockchain record may establish about CompletionPass #742 and at least four claims that still require outside evidence, authority, storage, identity verification, agreement, or recognition.
5. Explain why control of CompletionPass #742 would not automatically establish ownership of the certificate file, copyright, the learner's identity, course completion, or employer acceptance. Include the roles of metadata and authenticity.
6. Compare the proposed tokenized system with an alternative that uses ordinary payments and a signed certificate stored in a conventional credential database. Identify one possible benefit and two limitations of each approach. Then recommend the next investigation step before the providers choose a design, and explain your reasoning.

COMPLETION CHECK

Before moving to Section 4, ask yourself whether you can:



- » Distinguish a blockchain network and its native asset from tokens created through smart contracts on that network.
- » Explain why a token's function or utility does not guarantee value, liquidity, rights, safety, or legal treatment.
- » Investigate a stablecoin by examining its reference asset, structure, reserves or collateral, issuer or program rules, redemption process, evidence, markets, and depeg risks.
- » Separate an NFT record from its metadata, referenced item or service, issuer authority, ownership claims, copyright, authenticity, storage, and recognition.
- » Compare a tokenized design with an ordinary database, signed document, membership account, or other simpler alternative.

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

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 3 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 3 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.



UNDERSTANDING WEB3

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.



UNDERSTANDING WEB3

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.



UNDERSTANDING WEB3**LESSON 14: HOW A BLOCKCHAIN TRANSACTION WORKS**

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational and Safety Boundary: This lesson provides general education about blockchain transactions. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, exchange, network, asset, company, or financial product. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson. Do not create, sign, or broadcast a real transaction for any course activity. 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 earlier lessons, I introduced the public treasury associated with the Prison Professors mission. The independent PP token community made activity connected with that treasury visible on BNB Smart Chain. A person can open a blockchain explorer such as BscScan and see records connected with the published address. That visibility can make a transaction look immediate: a line appears on a screen, a status is displayed, and a balance changes.

Behind that line is a sequence of decisions and network actions. Someone or some authorized system prepares an instruction. The instruction identifies a network, addresses, an action, and a fee. An authorized key signs it. A node receives it. The network checks it. A validator may include it in a block. The transaction may succeed or fail during execution. Confirmations develop, and the network eventually treats the record as final according to its rules.

I want you to understand that sequence because a transaction can be technically valid and still be a bad decision. A correct digital signature does not prove that the signer understood the request. A successful status does not prove that the address belonged to the intended person. A public record does not guarantee that an exchange or another company has credited an account. Technology can verify certain facts, but it cannot replace careful judgment.

The most important work often happens before authorization. A person should slow down, verify the network, examine the destination, understand the proposed action, review the fee, and decide whether the instruction matches the intended purpose.

Once a valid transaction is broadcast and finalized, changing the result may be difficult or impossible.

You can learn this process without using a device or moving an asset. The offline exercise asks you to arrange transaction stages and identify where errors can enter. The purpose is not to practice sending money. The purpose is to practice thinking in sequence.

PURPOSE AND ESSENTIAL QUESTION

Lesson 14 traces a blockchain transaction from preparation through authorization, network processing, confirmation, and final recordkeeping. It separates actions taken by a user or application from actions taken by nodes, validators, and the network.

Essential Question:

- » Why do verification and patience matter before and after a person authorizes a blockchain transaction?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Sequence the major stages of a blockchain transaction.
- » Explain the roles of addresses, digital signatures, fees, nodes, validators, confirmations, and finality.
- » Distinguish preparation, authorization, broadcast, validation, execution, inclusion, confirmation, and finality.
- » Identify common reasons a transaction may be delayed, rejected, fail during execution, or succeed in an unintended way.
- » Describe precautions that reduce address, network, fee, contract, and counterparty errors.

KEY TERMS

DIGITAL SIGNATURE

Definition: Cryptographic evidence created with a private key to authorize a specific digital message or transaction. A network can use the signature to check that the transaction was authorized by the key connected with the sending account. A valid signature does not prove the signer's identity, wisdom, ownership rights, or understanding of the transaction.

Sample sentence: The digital signature showed that the transaction was authorized by the required key, but it did not show why the signer approved it.

TRANSACTION FEE

Definition: A charge paid for network resources used to process a transaction. On many networks, the fee depends on the work requested, network demand, and fee settings. The fee is normally paid in the network's native asset, even when the transaction involves another token.

Sample sentence: The token transfer required a transaction fee in the network's native asset.

BROADCAST

Definition: To send a signed transaction to a network node so that it can be checked and relayed to other nodes. Broadcasting submits the instruction; it does not guarantee inclusion, success, or finality.

Sample sentence: After the wallet broadcast the signed transaction, the instruction entered the network's pending process.

VALIDATION

Definition: The process of checking whether a transaction follows network rules. Checks may include the signature, account sequence, available balance, fee requirements, transaction format, and rules governing the requested action.

Sample sentence: Validation rejected the instruction because it did not meet the network's requirements.

CONFIRMATION

Definition: Evidence that a transaction has been included in a block accepted by the network. Additional blocks or network votes may increase confidence that the record will remain part of the accepted history. The meaning of a confirmation differs by network.

Sample sentence: The organization waited for the required confirmation standard before updating its records.

FINALITY

Definition: The point at which a blockchain's rules provide strong assurance that an accepted transaction will not be reversed. Different networks reach or describe finality in different ways and on different schedules.

Sample sentence: The public record showed the transaction in a block, but the team followed its policy and waited for finality before relying on it.

MAIN LESSON

A TRANSACTION IS A SIGNED INSTRUCTION

People sometimes speak as if a digital asset travels through the internet like a package moving through the mail. That description can mislead. On a blockchain, a transaction is better understood as an instruction asking the network to update its shared state.

A simple instruction might ask the network to reduce the recorded balance associated with one account and increase the balance associated with another. A more complex instruction might call a function in a smart contract. It might transfer a token, record an approval, exchange one asset for another, vote in a governance process, or carry out another programmed action.

The instruction normally contains several fields. The exact fields differ by network and transaction type, but they may include:

- » The network on which the transaction is intended to operate.
- » A sending account or address.
- » A destination address, such as another account or a smart contract.
- » An amount or requested function.
- » Data that tells a smart contract what action is requested.
- » A transaction sequence or nonce that helps prevent duplication and preserves order.
- » A limit and price for network computation or other fee information.
- » A digital signature authorizing the completed instruction.

Some information can be prepared by a wallet or application. The user may see only a summary. That convenience creates a responsibility: the summary should be checked, and any unclear request should be treated cautiously. Signing an instruction that cannot be understood is sometimes called blind signing. A careful person does not assume that a button labeled “confirm” describes every effect.

STAGE 1: PREPARE THE INSTRUCTION

Preparation begins before a private key is used. A person, organization, wallet, exchange, or application assembles the proposed transaction.

At this stage, the preparer should identify:

- » The correct blockchain network.
- » The correct asset or smart contract.
- » The intended destination address.
- » The amount or requested action.
- » The estimated transaction fee and the native asset needed to pay it.
- » Any service fee or withdrawal fee charged outside the blockchain fee.
- » Any memo, destination tag, reference, or additional information required by the receiving service.

These details matter because the same-looking address may be used on more than one compatible network, while an exchange or service may support only one route. A transaction can succeed on the selected network and still fail to produce the intended result at the receiving service. That is not necessarily a network failure. It may be a network-selection or counterparty problem.

Fees also require care. On BNB Smart Chain, BNB is the native asset used to pay transaction fees. A person sending another token may still need enough BNB for the fee. A displayed estimate can change with network conditions or with the complexity of a smart-contract action. An estimate is not a promise.

STAGE 2: REVIEW BEFORE AUTHORIZATION

Review is the last ordinary opportunity to catch an error before signing. The reviewer should compare the proposed instruction with an independent, trusted source of information.

A careful review asks:

- » Am I using the intended network?
- » Does the destination match the verified address or service instructions?
- » Is the asset the intended asset, including the correct token contract when relevant?
- » Is the amount correct, including the decimal placement?
- » Does the application describe the action clearly?
- » Am I approving a transfer, a token allowance, a contract interaction, or something else?
- » Is the fee reasonable for the proposed action and current conditions?
- » Am I being pressured to act quickly or keep the transaction secret?

Copying and pasting can reduce typing errors, but it does not remove risk. Malicious software can replace a copied address. A familiar beginning and ending



are not always enough to establish that a long address is correct. When circumstances permit, a person should compare the complete address or use a trusted address-book process. Organizations should use written verification and approval rules rather than memory alone.

STAGE 3: AUTHORIZE WITH A DIGITAL SIGNATURE

After review, the authorized key holder may sign the transaction. The signature is created from the transaction data and the private key. The private key should remain secret; the signature can be shared with the network.

The signature performs an important but limited job. It allows the network to verify that the required key authorized that exact transaction data. If the transaction data changes after signing, the signature will no longer match.

The signature does not answer every question. It does not prove that the signer:

- » Is the legal owner of the asset.
- » Understood the contract interaction.
- » Was free from pressure or deception.
- » Used a secure device.
- » Chose the correct network or address.
- » Followed an organization's internal policy.
- » Made a financially wise decision.

This distinction connects with Lesson 13. Custody determines who can authorize. Transaction discipline determines how that authority is used.

STAGE 4: BROADCAST TO THE NETWORK

The signed transaction is sent to a node. The node performs initial checks and may relay the transaction to other nodes. On many networks, valid pending transactions wait in a transaction pool, sometimes called a mempool, until a validator or block producer selects them.

Broadcasting is not the same as completing. A wallet or service may display a transaction identifier, often called a transaction hash, soon after submission. That identifier helps people locate or discuss the transaction. It is not proof that the transaction has been included in a block, executed successfully, credited by a receiving company, or finalized.

A transaction may remain pending because network demand is high, the offered fee is unattractive, a required earlier transaction from the same account is still pend-



ing, a node has not relayed it widely, or a service has not actually broadcast the instruction. Some systems allow a pending transaction to be replaced with another transaction using the same sequence number and a different fee. The details vary, so a person should follow verified instructions from the relevant network or service rather than improvising.

STAGE 5: VALIDATE, EXECUTE, AND INCLUDE

Nodes and validators apply network rules. A transaction may be rejected before inclusion if its format, signature, sequence, balance, or fee does not meet those rules. A rejected transaction does not become part of the accepted blockchain history.

A validator may select a valid pending transaction and place it in a proposed block. For a simple transfer, execution may update balances. For a smart-contract interaction, the network executes the contract code with the supplied data.

Execution can succeed or fail. A contract may reject the request because a condition was not met. The transaction may run out of the allowed computational resource. An attempted token transfer may fail because the sending account lacks the token balance or permission required by the contract.

An included but failed transaction can still consume a transaction fee because the network performed work. On Ethereum-compatible networks, including BNB Smart Chain, the exact fee rules depend on the network and transaction. This is one reason a status of “failed” should not be confused with “nothing happened.” The intended state change may have been reversed, while a fee may still have been charged and a public record may still exist.

STAGE 6: READ THE RECEIPT AND CONFIRMATION STATUS

After inclusion, the network produces a transaction receipt or equivalent record. A block explorer may display information such as:

- » The transaction hash.
- » The block containing the transaction.
- » The sending and destination addresses.
- » The network fee.
- » Whether execution succeeded or failed.
- » Token-transfer events or other contract logs.
- » The number of later blocks or confirmations.

An explorer translates network data into a readable page. It is useful, but it is not the blockchain itself, and its labels can be misunderstood. A “success” status generally



means the network executed the requested instruction without a protocol-level failure. It does not prove that the recipient was correct, that an off-chain company credited the right account, that a token has value, or that the transaction served the mission.

For a transaction involving an exchange, custodian, merchant, or another service, two records may matter. The blockchain records the on-chain event. The company keeps its own account records and may require a memo, supported network, minimum amount, identity review, or a certain number of confirmations. A blockchain success does not force the company's internal system to credit an account immediately.

STAGE 7: WAIT FOR FINALITY AND RECONCILE THE RECORDS

Networks use different methods to decide when an accepted block should be treated as final. Some rely on additional blocks, some use validator votes, and some combine methods. BNB Smart Chain uses validator consensus and a fast-finality process. Exact validator counts, block times, and finality timing can change through network upgrades, so they should be checked against current official documentation before publication or operational use.

Patience matters between first inclusion and finality. A careful policy defines what evidence is sufficient before a person or organization relies on a transaction. That policy may depend on the network, value, risk, counterparty, and legal or organizational requirements.

After finality, responsible recordkeeping should reconcile several questions:

- » Did the intended transaction reach the intended network and address?
- » Did execution succeed?
- » What fee was charged?
- » Did any related token event occur?
- » Did the receiving service or internal ledger record the result?
- » Did the transaction follow the organization's approval and mission rules?

Finality answers a blockchain-history question. It does not answer every accounting, legal, tax, ownership, or ethical question.

APPLIED SCENARIO: A COMMUNITY TREASURY TRANSACTION

The independent PP token community has used BNB Smart Chain and a public treasury address associated with the Prison Professors mission. Imagine that a community tracker reports a new community-generated fee transaction connected with that treasury. This simplified teaching scenario does not describe or verify every rule in the token's smart contract, and it does not promote the token or any digital asset.

An observer might see a new entry on BscScan and say, “The donation is complete.” A more careful analysis separates the stages and the claims.

Preparation: A wallet, contract, or application assembled a transaction on BNB Smart Chain. The instruction identified addresses, data or value, and a fee paid in the network’s native asset.

Authorization: An authorized key produced the required digital signature. If a smart contract initiated part of the process, a prior signed transaction may have called the contract. The public record does not reveal the private key.

Broadcast and validation: A node received and relayed the signed instruction. Network participants checked that it followed BNB Smart Chain rules.

Execution and inclusion: A validator included the transaction in a block. The network executed the requested action and created a receipt showing success or failure.

Confirmation and finality: Later network acceptance increased confidence that the record would remain in the chain’s history.

Reconciliation: Observers could compare the public record with the published treasury address and community report. That comparison could support a limited statement about on-chain activity. It would not, by itself, prove the complete custody arrangement, every contract rule, donor identity, legal ownership, future value, internal accounting treatment, or mission compliance.

This example connects technical discipline with credibility. If I describe the public treasury, I should state what the blockchain evidence supports and avoid claiming more. Participants can practice the same habit in their own work: identify the evidence, trace the sequence, and separate a verified fact from an assumption.

Delays, Failures, and Successful Mistakes

Not every problem has the same meaning. A careful learner distinguishes four categories.

DELAYED OR PENDING

The signed transaction has been submitted but has not yet reached the required inclusion or confirmation status. Possible causes include network demand, fee settings, sequence conflicts, node problems, or a service delay.

REJECTED BEFORE INCLUSION

The network or submitting service refuses the transaction before it enters an accepted block. Possible causes include an invalid signature, incorrect format, insuf-

ficient balance for the amount and fee, an invalid sequence, or fee settings that do not meet network requirements.

INCLUDED BUT FAILED DURING EXECUTION

The transaction enters a block, but the requested state change does not complete. A smart contract may reject the action, or the transaction may exhaust its computational allowance. The public record may show failure, and a network fee may still be charged for work performed.

TECHNICALLY SUCCESSFUL BUT UNINTENDED

The network executes exactly what was signed, but the signer chose the wrong address, wrong network, wrong token, wrong amount, harmful contract approval, or dishonest counterparty. The blockchain may show success even though the human purpose failed.

That final category is especially important. Network validation checks protocol rules. It does not guarantee good judgment.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

BENEFITS OF A TRACEABLE TRANSACTION PROCESS

- » A digital signature can link authorization to a specific key without revealing the private key.
- » Shared network rules allow independent nodes to check the transaction.
- » A transaction hash and public record can support tracking and reconciliation.
- » Confirmations and finality provide increasing assurance that accepted history will remain stable.
- » Organizations can use written approval and verification procedures around the technical process.

IMPORTANT LIMITATIONS AND RISKS

- » A valid signature can authorize a harmful or misunderstood instruction.
- » An address usually does not identify a human being by itself.
- » Transactions may be irreversible after finality.
- » Fees may change, and failed execution may still consume a fee.
- » Smart-contract actions may have effects that a simple wallet summary does not explain.
- » A blockchain record may not match an exchange, merchant, court, accounting system, or organization's internal record.

- » A public transaction can expose patterns that affect privacy.
- » Compatible-looking networks and tokens can create routing and identification errors.

COMMON MISCONCEPTIONS

- » “Broadcast means complete.” Broadcast means that a signed instruction was submitted to a node; it may still be pending, rejected, replaced, or dropped.
- » “A transaction hash proves success.” A hash identifies a transaction. Its receipt and status must still be checked.
- » “One confirmation always means final.” Networks define confirmation and finality differently.
- » “Success means the intended person received the asset.” Network success proves execution under protocol rules, not human identity or intent.
- » “A failed transaction costs nothing.” An included transaction that fails during execution may still consume a fee.
- » “The fee is paid in whatever token I am sending.” Many networks require the fee in their native asset.
- » “The blockchain will correct a wrong address.” A valid transaction can succeed at an unintended address.
- » “A block explorer is customer support.” An explorer displays public data; it generally cannot reverse a transaction or control an account.

OFFLINE EXERCISE: PUT THE TRANSACTION IN ORDER

Estimated time: 25–30 minutes

Materials: Separate paper and a pencil.

The eight cards below are deliberately out of order. Do not create an account or perform a real transaction. On separate paper, write the letters in the order that best represents a typical blockchain transaction.

TRANSACTION-STAGE CARDS

Card A: A validator includes the transaction in a block and the network executes the requested action.

Card B: The preparer or reviewer checks the network, address, asset, amount, action, and estimated fee.

Card C: The authorized key creates a digital signature for the completed transaction data.

Card D: A node receives the signed transaction and relays it to the network.

Card E: The accepted record gains confirmations and reaches the network's finality standard.

Card F: A wallet, application, contract, or service assembles the proposed transaction fields.

Card G: Network participants check the signature, sequence, balance, fee, format, and other protocol rules.

Card H: A receipt or explorer record shows the block, fee, and success or failure status.

After arranging the cards, complete these tasks:

1. Identify one error that could enter during preparation or review.
2. Identify one risk that a valid digital signature cannot prevent.
3. Explain why broadcasting does not prove success.
4. Explain the difference between a rejected transaction and an included transaction that fails during execution.
5. Explain why a technically successful transaction may still fail its human purpose.
6. Identify what an organization should verify when reconciling an on-chain transaction with its internal records.
7. Write one sentence explaining why patience matters after the first confirmation.

Important limitation of the exercise: The cards describe a simplified, typical process. Networks, layers, wallets, custodians, smart contracts, and services may combine, reorder, or label stages differently. The exercise teaches reasoning, not an operational procedure.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. What does a digital signature establish most directly?
 - a. That the signer made a wise decision
 - b. That the required private key authorized the specific transaction data
 - c. That the destination belongs to the intended person
 - d. That the transaction is already final
2. Which statement best describes broadcast?



- a. The transaction has been submitted to a network node, but inclusion and success are not guaranteed
 - b. The transaction has reached finality
 - c. The recipient's company has credited an internal account
 - d. The fee has been refunded
3. Which situation can appear as successful on-chain while still failing the signer's purpose?
- a. A node rejects a transaction with an invalid signature
 - b. A wallet has not yet assembled an instruction
 - c. A valid transaction sends an asset to the wrong address
 - d. A learner completes the exercise on paper

TRUE OR FALSE

- » If a transaction is included in a block but fails during smart-contract execution, a network fee may still be charged for the work performed.

SHORT EXPLANATION

- » In three or four sentences, explain why a transaction hash and a success status do not prove that every human, business, legal, or ethical purpose was satisfied.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A blockchain transaction is a signed instruction asking a network to update its shared state.
- » Preparation identifies the network, address, asset, amount, action, and fee.
- » Review is the last ordinary opportunity to catch many errors before authorization.
- » A digital signature proves authorization by a key, not identity, wisdom, ownership, or freedom from deception.
- » Broadcast submits a signed transaction to a node; it does not guarantee inclusion, success, or finality.
- » Validation checks protocol rules such as signature, sequence, balance, format, and fee requirements.
- » A validator may include a transaction in a block and execute the requested action.
- » A rejected transaction, a pending transaction, an included failure, and a successful mistake are different outcomes.



- » An included transaction that fails during execution may still consume a transaction fee.
- » A transaction hash helps locate a transaction but does not prove success.
- » Confirmation and finality have network-specific meanings.
- » A blockchain success does not guarantee that an exchange, merchant, or other counterparty has updated its own records.
- » BNB Smart Chain uses BNB for transaction fees, including transactions involving other tokens.
- » The Prison Professors community treasury example shows how public evidence can support a limited claim without proving every private or off-chain fact.
- » Verification, patience, reconciliation, and honest communication strengthen credibility.
- » No course exercise requires a real account, wallet, asset, or transaction.

The practical lesson is simple: slow down before signing, identify what each stage proves, and do not confuse technical success with complete human success.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- » Explain in your own words what a blockchain transaction is.
- » Sequence the major stages from preparation through finality.
- » Describe what a digital signature proves and what it does not prove.
- » Explain why a transaction hash, confirmation, and finality are different.
- » Identify one address or network error and one fee or smart-contract error that careful review may reduce.
- » Explain the difference between a rejected transaction, an included failure, and a technically successful mistake.
- » Use the Prison Professors community treasury example to distinguish on-chain evidence from custody, accounting, ownership, or mission claims.
- » Explain why verification and patience matter before and after authorization.
- » Connect transaction discipline with responsibility, credibility, preparation, or trust.



Your response should demonstrate reasoning. Do not create, sign, or broadcast a transaction. Do not include any real password, private key, seed phrase, authentication code, account number, wallet address, balance, transaction hash, or transaction detail.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 14: How a Blockchain Transaction Works, 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 14 — [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 hashes, transaction details, or other sensitive credentials.

TECHNICAL AND SAFETY CONTEXT REVIEWED JULY 22, 2026.

1. Prison Professors. Understanding Web3 — Course Blueprint, Version 1.1, July 2026; Lesson 12: Wallets, Addresses, Keys, and Seed Phrases, approved Draft Version 0.1; Lesson 13: Custody and Self-Custody, approved Draft Version 0.2; and project direction I supplied for this course. Controlling sources for the lesson requirements, first-person voice, community-treasury case, offline design, submission process, and sensitive-information boundaries.
2. Ethereum.org. “Transactions,” updated March 12, 2026; accessed July 22, 2026. Used for the signed-instruction model, transaction fields, broadcast, pending pool, validator inclusion, and lifecycle explanation. <https://ethereum.org/developers/docs/transactions/>
3. Ethereum.org. “Ethereum Gas and Fees: Technical Overview,” updated June 24, 2026; accessed July 22, 2026. Used for computational-resource explanations, fee purpose, unused gas, and the distinction between rejection before inclusion and failure during execution. <https://ethereum.org/developers/docs/gas/>



4. BNB Chain. “BNB Smart Chain Introduction” and “BNB Smart Chain Quick Guide”; accessed July 22, 2026. Used for BNB Smart Chain’s validator-based processing, fast-finality context, Ethereum compatibility, and BNB as the native transaction-fee asset. Exact network parameters are time-sensitive and should be reverified before publication. <https://docs.bnbchain.org/bnb-smart-chain/introduction/> and <https://docs.bnbchain.org/bnb-smart-chain/developers/quick-guide/>



UNDERSTANDING WEB3

LESSON 15: SCAMS, SECURITY, PRIVACY, AND IRREVERSIBLE ERRORS

A Prison Professors Self-Directed Course

Estimated time: 70–105 minutes

Educational and Safety Boundary:

This lesson provides general education about scams, security, privacy, and digital-asset transactions. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, exchange, network, asset, company, or financial product. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson. Do not contact anyone, open a link, create an account, share personal information, or perform a transaction for any course activity. 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

Throughout my years in prison, I learned to slow down before making a decision that could shape my future. Pressure can narrow a person's attention. Excitement can do the same. When someone promises an easy solution, demands immediate action, or asks for secrecy, disciplined thinking becomes a form of protection.

Web3 gives people new ways to exchange value, coordinate communities, and verify public records. The same tools can also be used in dishonest schemes. A scammer may pretend to represent a company, a public figure, a support team, a charity, or a person we trust. The message may look professional. It may use familiar names and accurate public information. It may even point to a real blockchain transaction. None of those features proves that the request is legitimate.

In earlier lessons, I described the independent PP token community and the public treasury associated with the Prison Professors mission. Public blockchain records can help people observe activity connected with a published address. Yet visibility does not prevent impersonation. A dishonest person could copy our name, logo, public address, or community language and then ask someone to send funds, reveal credentials, or visit a false support page. A copied identity is not the same as verified authority.

I encourage you to build a repeatable response before you ever face such a request. Stop. Verify. Seek help. Those three actions create time and distance between an emotional message and an irreversible decision. They also apply beyond Web3—to

employment offers, family emergencies, charitable requests, account warnings, and other claims that arrive through digital communication.

You can practice this judgment without a device. In the offline exercise, you will examine fictional messages, mark warning signs, and explain a safe response. You will not use a working link, contact a sender, disclose information, or move any asset.

PURPOSE AND ESSENTIAL QUESTION

Lesson 15 explains how manipulation can lead a person to reveal sensitive information or authorize an unwanted transaction. It presents common scam patterns, shows how public blockchain records affect privacy, and teaches a cautious response that does not depend on technical expertise.

Essential Question:

- » How can a person slow down, verify a digital claim, and protect sensitive information before an error becomes difficult or impossible to reverse?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Recognize common patterns in phishing, impersonation, investment, giveaway, romance, support, and recovery scams.
- » Identify warning signs such as pressure, secrecy, guaranteed returns, credential requests, and unsolicited contact.
- » Explain how public blockchain records can affect personal privacy.
- » Describe why some blockchain transactions are difficult or impossible to reverse.
- » Apply a Stop, Verify, Seek Help process without visiting a link, sharing credentials, or performing a real transaction.

KEY TERMS

PHISHING

Definition: A deceptive attempt to obtain sensitive information or cause a harmful action by pretending to be a trustworthy person or organization. A phishing message may arrive by email, text, social media, telephone, letter, or another channel.

Sample sentence: The unexpected account warning was a phishing attempt designed to make the recipient open a false sign-in page.



IMPERSONATION

Definition: Pretending to be another person or organization in order to gain trust, information, money, or access. An impersonator may copy a name, photograph, logo, writing style, or public address.

Sample sentence: The copied logo did not prove that the message came from the organization it claimed to represent.

SOCIAL ENGINEERING

Definition: The use of deception, pressure, emotion, or trust to influence a person into revealing information or taking an action. Social engineering attacks people's decisions rather than relying only on a technical weakness.

Sample sentence: The caller used social engineering by creating fear and demanding immediate secrecy.

RECOVERY SCAM

Definition: A scheme in which someone promises to recover money, digital assets, or access lost in an earlier scam, usually in exchange for an advance fee, credentials, or additional payment.

Sample sentence: The person who promised a guaranteed refund for an advance fee was attempting a recovery scam.

PRIVACY

Definition: A person's ability to control or limit access to information about identity, activity, relationships, location, finances, or other personal circumstances. Privacy on a public blockchain is limited because transaction records can often be viewed and analyzed.

Sample sentence: Reusing one public address can reduce privacy by making separate transactions easier to connect.

IRREVERSIBLE TRANSACTION

Definition: A transaction that cannot ordinarily be canceled or reversed after the network accepts and finalizes it. A recipient may voluntarily return funds, but the blockchain usually does not provide a customer-service button that forces a refund.

Sample sentence: The irreversible transaction left little opportunity to correct the wrong destination after finality.



MAIN LESSON

SCAMS TARGET DECISIONS

A scam does not always begin with a technical attack. It often begins with a story.

The story may say that an account will close, a family member faces an emergency, an investment opportunity will disappear, a prize is waiting, a public figure needs support, or a lost payment can be recovered. The sender then gives the recipient a narrow path: act now, keep the conversation private, follow these instructions, and do not verify the claim elsewhere.

The story changes, but the structure often remains familiar:

- » Establish trust by using a recognizable name, role, logo, relationship, or shared interest.
- » Create emotion through fear, hope, urgency, affection, authority, or embarrassment.
- » Reduce independent thinking by demanding speed or secrecy.
- » Request value, information, access, or authorization.
- » Discourage verification through an established, independent channel.

This structure is social engineering. It exploits ordinary human reactions. Intelligent and experienced people can be deceived when a message reaches them at the wrong time or creates the right emotion. Shame after an error can then keep a victim from asking for help, which gives the scammer more control.

A safer response treats emotional intensity as a signal to pause. The stronger the pressure, the more valuable an independent check becomes.

PHISHING: A FALSE PATH TO INFORMATION OR ACTION

Phishing messages often imitate a bank, exchange, wallet provider, employer, government office, delivery service, charity, or familiar contact. A message may claim that an account has a problem and provide a link or telephone number. The destination may be designed to capture a password, authentication code, seed phrase, identity document, or payment.

Some phishing messages contain obvious errors. Others are polished. Artificial intelligence and copied public information can help a criminal create convincing language, images, audio, or video. A professional appearance cannot establish authenticity.

COMMON WARNING SIGNS INCLUDE:

- » An unexpected message about an account, payment, prize, refund, or emergency.
- » A request to open a link or attachment before the claim can be checked.
- » A sender address, telephone number, or account name that is slightly different from the official one.
- » A demand for a password, private key, seed phrase, authentication code, or remote access.
- » A threat that delay will cause immediate loss, arrest, closure, or public embarrassment.
- » Instructions to bypass ordinary policies or keep the communication secret.

Do not use the contact information supplied in a suspicious message to verify that same message. A false sender can also provide a false support number. Use a known statement, printed policy, official directory, previously verified record, or another independent source.

IMPERSONATION AND FALSE SUPPORT

Impersonation can occur anywhere people communicate. A dishonest account may copy the name and photograph of a founder, celebrity, nonprofit leader, family member, or support representative. It may reply beneath a genuine public post so that the false account appears connected with the real one.

False support agents often look for people who publicly describe a problem. The agent may offer help and then request a seed phrase, private key, screen-sharing session, software installation, or payment to “validate” a wallet. A legitimate service does not need a seed phrase or private key to provide ordinary support. Anyone who receives those credentials can control the associated assets.

Authority should be verified through an established channel. A badge, username, logo, photograph, or confident tone is only part of a presentation. It is not proof of identity.

INVESTMENT AND GUARANTEED-RETURN SCAMS

An investment scam may begin with an unsolicited message, an online relationship, a group conversation, or a convincing-looking platform. The promoter may display supposed profits and allow a small early withdrawal to build confidence. Later, the victim may be asked to deposit more or pay a fee, tax, or security charge before withdrawing. Additional payment can deepen the loss.

WARNING SIGNS INCLUDE:

- » Guaranteed profits or unusually high returns with little or no risk.
- » Claims that a secret system, automated program, insider connection, or famous supporter removes uncertainty.
- » Pressure to act before research or independent advice is possible.
- » Instructions to buy or transfer a specific digital asset to an unfamiliar address.
- » A dashboard showing profits that cannot be independently withdrawn or verified.
- » A demand for new money to release existing funds.

Every investment involves uncertainty. A person who guarantees a return or claims that risk has disappeared is withholding a central truth. Public excitement, a rising price, or a large community does not establish safety, legality, liquidity, or future value.

GIVEAWAY AND ADVANCE-PAYMENT SCAMS

A giveaway scam may claim that a public figure, company, or community will send back more digital assets than the recipient sends first. The scammer may display copied videos, false comments, or a public address that appears active.

A legitimate gift does not require a person to send value first in order to receive a larger amount. A transaction on a block explorer only proves that a transaction occurred. It does not prove that the promotion is honest, that displayed participants are independent, or that a repayment will follow.

Advance-payment schemes use the same logic in other forms. A person may be told to pay a processing charge to receive a prize, grant, inheritance, job, loan, refund, or charitable distribution. The promised benefit becomes a reason to send money before the claim has been verified.

ROMANCE AND RELATIONSHIP-BASED SCAMS

A romance scam develops trust over time. The person may offer attention, affection, spiritual connection, friendship, or plans for a future together. The request for money may come later and may involve travel, medical care, legal trouble, business, or an investment opportunity.

The relationship can feel real because the emotional experience is real for the victim. That does not establish that the other identity or story is genuine. A refusal to meet through a safe, verifiable process; repeated emergencies; requests for secrecy; or pressure to send digital assets should trigger a pause and independent support.

Relationship-based manipulation is not limited to romance. It can involve friendship, mentorship, employment, shared faith, shared incarceration experience, or commitment to a mission. Trust should grow alongside verification, not replace it.

RECOVERY SCAMS CAN FOLLOW THE FIRST LOSS

After a scam, a victim may search for help or post publicly about the loss. A recovery scammer then claims to be a lawyer, investigator, government agent, blockchain expert, hacker, or recovery service. The new scammer may already know details about the first loss and use that knowledge to sound credible.

The recovery offer may require an advance fee, a new deposit, access to an account, or sensitive credentials. It may promise certainty even when the original transfer is irreversible. Paying again can create a second loss.

No private person can force a public blockchain to reverse a finalized transaction. Law enforcement, courts, exchanges, insurers, or other institutions may have lawful processes in some circumstances, but no outcome is guaranteed. A person seeking help should use verified official channels and should not provide credentials or new payments to an unsolicited rescuer.

WARNING SIGNS SHOULD BE CONSIDERED TOGETHER

One unusual detail does not always prove fraud. A legitimate organization may have a deadline. A family member may face a real emergency. A new company may contact a potential customer. The correct response is not automatic disbelief; it is verification proportional to the risk.

Several warning signs together increase concern:

- » The contact was unexpected.
- » The sender creates urgency or fear.
- » The sender requests secrecy.
- » The claim promises guaranteed returns, certain recovery, or easy income.
- » Payment must be made in digital assets, gift cards, wire transfer, or another hard-to-reverse method.
- » The sender requests a password, private key, seed phrase, authentication code, or remote access.
- » The sender provides the only method for verifying the claim.
- » The explanation changes when questions are asked.
- » The sender discourages consultation with family, staff, counsel, or an independent professional.

- » More money is required to release funds that supposedly already belong to the recipient.

STOP, VERIFY, SEEK HELP

I recommend a three-part response whenever a digital claim involves money, credentials, identity, access, or urgency.

STOP

Do not reply immediately. Do not open the supplied link, call the supplied number, install software, share a code, or send a payment. If possible, preserve the message without forwarding sensitive information. Time allows emotion to settle and gives reason a chance to return.

Ask: What action is the sender trying to cause? What could I lose if the request is false? Why must I act now?

VERIFY

Check the claim through a channel that the sender did not control. Use previously verified contact information, an official printed statement, a known family contact, an established organizational procedure, or another independent source. Compare more than the display name. Verify the identity, authority, purpose, destination, and requested action.

For a Web3 claim, verification may include checking official documentation, confirming a published address through more than one trusted source, examining what a smart-contract request would authorize, and confirming that the network matches the intended service. A block explorer can support limited verification of public transaction data. It cannot prove the human identity behind every address or the truth of an off-chain promise.

SEEK HELP

Ask a trusted person to review the claim before acting. Depending on the situation, that person may be a family member, institutional staff member, attorney, financial professional, organization representative, law-enforcement contact, or experienced technical professional reached through a verified channel.

Seeking help is a sign of disciplined judgment. A second person may notice pressure, inconsistency, or a hidden assumption that the recipient missed. If a possible scam has already caused a loss, prompt reporting may preserve records and improve the chance that an appropriate institution can respond, even though recovery is not guaranteed.

SECURITY PRACTICES SUPPORT CAREFUL JUDGMENT

Good security does not eliminate deception, but it reduces the opportunities available to an attacker.

USEFUL PRACTICES INCLUDE:

- » Use a strong, unique password for each important account.
- » Use multifactor authentication when available, and protect authentication codes.
- » Keep devices and software updated through trusted channels.
- » Store backups of essential information according to a secure, documented plan.
- » Limit the personal information posted publicly.
- » Review account activity and public addresses without revealing credentials.
- » Follow written approval and verification procedures for organizational funds.
- » Contact support through an established official path, not through an unsolicited message.

Never share a private key or seed phrase. Do not photograph it for convenience, enter it into an unfamiliar site, send it through email or messaging, or give it to a support representative. A person who receives it may be able to control the associated assets without further permission.

PUBLIC RECORDS AND PERSONAL PRIVACY

Public blockchains are often described as transparent. Depending on the network, a person may be able to view addresses, amounts, token movements, smart-contract interactions, fees, and timing. The record may use an address rather than a legal name, but an address is not automatically anonymous.

An address can become connected with a person or organization through a public post, exchange record, court document, donation page, purchase, data leak, or repeated pattern of activity. Once one connection is known, analysts may compare related transactions and infer relationships or habits. Some inferences will be accurate; others may be wrong.

Reusing one address can make activities easier to connect. Publishing a balance can attract unwanted attention. Combining blockchain data with social-media posts, location information, or other public records can reveal more than any single source.

Privacy therefore requires judgment about disclosure. Do not place real addresses, balances, transaction hashes, account details, or credentials in a course assignment. An organization that publishes a treasury address for transparency should still

avoid revealing private keys, signer identities, device details, backup locations, or procedures that could weaken security.

Transparency and privacy can serve different purposes. A public treasury may support accountability by allowing people to observe certain on-chain activity. The same public record does not reveal every fact about identity, ownership, custody, accounting, intent, or mission use. Responsible communication states what the evidence supports and leaves unsupported claims unstated.

WHY IRREVERSIBILITY CHANGES THE DECISION

Many familiar payment systems have an institution that may pause, dispute, or reverse a transaction under defined rules. A public blockchain usually works differently. After a valid transaction is accepted and finalized, the network generally does not have a central operator who can cancel it because the sender was deceived or chose the wrong address.

The recipient can voluntarily send value back. An exchange may freeze an account under its rules or legal obligations. Law enforcement may investigate. A court may issue an order. None of those possibilities changes the original blockchain record automatically, and none guarantees recovery.

Irreversibility shifts protection toward the period before authorization. The sender should verify the network, destination, asset, amount, action, fee, counterparty, and purpose before signing. A small test transaction may reduce some operational risk in real-world settings, but this course does not ask anyone to conduct one. A test also cannot prove that a counterparty is honest or that a later request is safe.

An urgent message and an irreversible payment method are a dangerous combination. Stop, Verify, Seek Help creates a protective barrier before the network records the decision.

APPLIED SCENARIO: A FALSE PRISON PROFESSORS REQUEST

The following scenario is fictional. It does not describe a verified incident, and it does not reproduce a working address, account, link, or message.

Imagine that a person receives a message from an account displaying the Prison Professors name and logo. The sender refers to the independent PP token community and the public treasury on BNB Smart Chain. The message says that a new “treasury verification program” will double any contribution sent within one hour. It provides an address and says that participants should keep the opportunity private until the verification period closes.

PRISON PROFESSORS CHARITABLE CORPORATION

Prison Professors Charitable Corporation / 1205 BMC Drive / Suite #706 / Cedar Park, TX 78613
IRS 501c3 #85-2603315 / www.PrisonProfessors.org



The message uses real public ideas: Prison Professors has a mission, an independent community created a token, and a public treasury address has been discussed. Those facts do not authenticate the new request.

THE WARNING SIGNS INCLUDE:

- » Unsolicited contact.
- » A copied organizational identity.
- » A guaranteed return.
- » A one-hour deadline.
- » A request for secrecy.
- » A hard-to-reverse payment.
- » Verification instructions controlled by the sender.

A cautious recipient would stop without replying or sending value. The recipient would verify the claim through established Prison Professors information, such as previously confirmed contact details, rather than any link or number in the message. The recipient could seek help from a trusted person and report the impersonation through an official channel.

If I communicate about the Prison Professors mission, I want people to distinguish our work from independent community activity and from anyone who copies our identity. Prison Professors did not organize, manage, or control the PP token project. Public support for a mission does not give every supporter authority to speak for the organization. Future lessons may continue using the community project as a teaching example, but no course lesson asks a participant to buy a token, send funds, contact a community member, or perform a transaction.

The broader lesson applies to every participant building a Profile. Consistent work can earn attention and support from people we do not yet know. That opportunity also creates a responsibility to protect our name, verify claims, document decisions, and communicate honestly about who has authority.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

BENEFITS OF A DISCIPLINED SECURITY PROCESS

- » A pause reduces the influence of urgency, fear, excitement, and embarrassment.
- » Independent verification separates a sender's claim from evidence controlled by the sender.
- » A second reviewer may identify inconsistencies or risks that one person missed.



- » Written procedures help organizations apply the same safeguards repeatedly.
- » Limited disclosure reduces the information available for impersonation and targeted attacks.
- » Prompt reporting can warn others and preserve evidence for an appropriate institution.

IMPORTANT LIMITATIONS AND RISKS

- » A polished message, copied logo, public transaction, or familiar name can still be deceptive.
- » Public blockchain records may expose patterns without identifying the full human context.
- » An address does not prove who controls it or why a transaction occurred.
- » A valid digital signature can authorize a decision made under deception or pressure.
- » Finalized transactions may be difficult or impossible to reverse.
- » Recovery is uncertain, and a recovery offer can be a second scam.
- » Privacy cannot be restored fully after sensitive information becomes public.
- » Security tools are less effective when a person voluntarily reveals credentials or bypasses a warning.

COMMON MISCONCEPTIONS

“Only careless people are scammed.” Scammers design stories around ordinary emotions and trusted relationships. A repeatable process protects people across experience levels.

“A professional-looking message is authentic.” Appearance can be copied. Verify identity and authority through an independent channel.

“A public blockchain proves the entire story.” It can show certain on-chain records, but it does not establish every identity, promise, ownership claim, or off-chain event.

“Support needs my seed phrase to fix the problem.” Anyone with the seed phrase may gain control. Ordinary support should not request it.

“A guaranteed return removes risk.” Guarantees of high or certain profit are a major warning sign.

“Paying one more fee will release my funds.” New fees can extend an investment, withdrawal, or recovery scam.



“A verified social-media badge proves the request is safe.” Accounts can be copied, compromised, or misunderstood. Verify the specific request elsewhere.

“The blockchain will refund an accidental transfer.” A finalized network record usually has no forced-refund feature.

“Privacy means hiding wrongdoing.” Lawful privacy protects safety, identity, relationships, and personal autonomy. It can coexist with appropriate accountability.

OFFLINE EXERCISE: MARK THE WARNING SIGNS

Estimated time: 30–35 minutes

Materials: Separate paper and a pencil.

The five messages below are fictional. They contain no working link, real address, telephone number, or account. Do not contact anyone or perform any action described. For each message, complete four tasks:

1. Identify at least two warning signs.
2. Name the emotion or form of pressure the sender may be using.
3. Write a safe response using Stop, Verify, Seek Help.
4. Identify one piece of information that should never be disclosed.

MESSAGE A: URGENT ACCOUNT WARNING

“Security Department: Your account will close in 20 minutes. Confirm your password and six-digit code on the attached page. Failure to respond will permanently lock your funds.”

MESSAGE B: FAMOUS SUPPORTER GIVEAWAY

“A well-known Web3 founder is rewarding the first 50 supporters. Send one token now and receive two back. This private offer has been verified on the blockchain. Do not share it until you receive your reward.”

MESSAGE C: FRIENDLY INVESTMENT COACH

“I have enjoyed our conversations, and I want us to build a future. My trading system has never lost. Deposit more today so your balance can qualify for withdrawal. The tax must be paid in advance.”

MESSAGE D: WALLET SUPPORT

“I saw your public post about a missing transaction. I am an official recovery technician. Send your seed phrase so I can reconnect the wallet. My service charge is due after I confirm access.”

MESSAGE E: MISSION IMPERSONATION

“The Prison Professors treasury needs immediate verification. Send a contribution to the address below within one hour and it will be doubled. Keep the address private while the audit is active.”

After reviewing all five messages, answer these questions:

- » Which warning sign appeared most often?
- » Which message might be most persuasive to you, and why?
- » How can public information make an impersonation attempt more convincing?
- » Why should a person avoid the telephone number or link supplied in a suspicious message?
- » How does transaction irreversibility increase the value of pausing before authorization?
- » Write a three-sentence personal rule you could use when a digital claim creates urgency.

Important limitation of the exercise: A warning sign is a reason to investigate, not automatic proof that every claim is false. The safe response is to pause and verify through an independent channel without disclosing information or sending value.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which request is the clearest sign of a dangerous support impersonation?
 - a. A suggestion to read public documentation
 - b. A request for a seed phrase or private key
 - c. A reminder to keep software updated
 - d. A recommendation to ask a trusted person for help
2. What is the safest way to verify an unexpected account warning?
 - a. Use the link in the message because it is faster
 - b. Reply and ask the sender whether the message is genuine
 - c. Contact the organization through previously verified information

- d. Forward the password so support can compare it
- 3. What can a public blockchain record establish most directly?
 - a. Every human identity and motive connected with a transaction
 - b. That an investment promise is honest
 - c. Certain on-chain activity recorded under the network's rules
 - d. That a recipient will voluntarily return a payment

TRUE OR FALSE

- » After a finalized blockchain transaction, a sender can ordinarily require the network to reverse it through a customer-service request.

SHORT EXPLANATION

- » In three or four sentences, explain how Stop, Verify, Seek Help can protect a person from an urgent impersonation request.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Scams often use trust, emotion, urgency, and secrecy to influence a decision.
- » Phishing imitates a trusted source to obtain information or cause a harmful action.
- » Impersonators may copy names, logos, photographs, public addresses, and accurate public facts.
- » Social engineering targets human judgment as well as technical systems.
- » Guaranteed returns, unsolicited contact, credential requests, and advance payments are strong warning signs.
- » A romance or relationship scam can build trust for weeks or months before requesting value.
- » Recovery scammers often target people who have already experienced a loss.
- » Never share a password, private key, seed phrase, or authentication code.
- » Stop before replying, opening a supplied link, calling a supplied number, or sending value.
- » Verify through an independent channel that the sender did not control.
- » Seek help from a trusted person or appropriate institution before acting.
- » Public blockchain records can support limited on-chain claims but do not prove every identity, promise, or off-chain event.
- » A public address is not automatically anonymous, and repeated activity can reveal patterns.

- » Finalized blockchain transactions may be difficult or impossible to reverse.
- » The fictional Prison Professors example shows how real public information can be copied into a false request.
- » No course exercise requires internet access, an account, a wallet, a digital asset, or a real transaction.

The practical lesson is simple: create distance between pressure and authorization. Stop. Verify. Seek help.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- » Describe why a scam can persuade an intelligent person.
- » Explain the roles of urgency, secrecy, trust, fear, hope, or affection in social engineering.
- » Identify three warning signs that would cause you to pause.
- » Explain how you would apply Stop, Verify, Seek Help to an unexpected digital claim.
- » Describe one independent verification channel you could use without following the sender's instructions.
- » Explain why a seed phrase, private key, password, or authentication code must remain confidential.
- » Explain how public blockchain records can support transparency while reducing privacy.
- » Describe why transaction irreversibility increases the need for review before authorization.
- » Use the fictional Prison Professors impersonation scenario to distinguish a real mission from an unauthorized request.
- » State the personal rules you will follow to slow down and verify future claims.

Your response should demonstrate reasoning and personal responsibility. Do not open a link, contact a sender, create an account, share personal information, or perform a transaction. Do not include any real password, private key, seed phrase, authentication code, account number, wallet address, balance, transaction hash, transaction detail, or other sensitive information.



SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 15: Scams, Security, Privacy, and Irreversible Errors, and the date you completed the entry.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 15 — [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 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 hashes, transaction details, or other sensitive credentials.

UNDERSTANDING WEB3**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.

UNDERSTANDING WEB3**LESSON 16: SMART CONTRACTS AND DECENTRALIZED APPLICATIONS**

A Prison Professors Self-Directed Course

Estimated time: 70–105 minutes

Educational and Safety Boundary:

This lesson provides general education about smart contracts, decentralized applications, and related risks. It does not provide individualized financial, investment, legal, tax, or programming advice. No activity requires internet access, an account, a wallet, a digital asset, programming, or a transaction.

OPENING GUIDANCE

While serving 26 years in federal prison, I relied on self-directed learning because I could not access the changing technology outside. I learned by reading, developing a vocabulary, writing about new ideas, and documenting my progress. That process taught me to examine how a system works instead of being impressed by a label.

The term smart contract can sound more powerful than it is. The word smart may suggest that the code can think. The word contract may suggest that every program creates a legally enforceable agreement. Neither conclusion is reliable. A smart contract is computer code deployed on a blockchain. It follows the instructions written into it when a person, another program, or an outside service triggers the relevant function.

This lesson connects the earlier lessons on blockchains, tokens, wallets, transactions, and safety. A token on BNB Smart Chain or Ethereum is often created and managed through smart-contract code. A decentralized application may give a person a website or other interface for interacting with that code. The visible screen is only one part of the system.

The independent PP token community gives us a recurring example. Neither Prison Professors nor I created, organized, managed, or controlled that token project. Community members used a smart contract on BNB Smart Chain to create a token with programmed fee behavior. That code can perform defined calculations and record results. It cannot decide whether a mission deserves support, whether a public claim is complete, or whether a human decision is wise.

I encourage you to ask two questions throughout this lesson: What can the code do, and what still depends on people? Those questions will help you evaluate any proposed blockchain application without accepting advertising language as proof.

PURPOSE AND ESSENTIAL QUESTION

Lesson 16 explains how code can carry out defined actions on a blockchain and how people may interact with that code through decentralized applications. It also shows why automated execution does not remove coding defects, faulty data, administrative control, confusing interfaces, legal uncertainty, or the need for human judgment.

Essential Question:

- » What can smart-contract code automate, and which decisions still require human judgment, evidence, governance, and accountability?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define smart contract and decentralized application in plain language.
- » Explain why a smart contract is code rather than an intelligent decision-maker or automatic legal agreement.
- » Trace a simple input–rule–output process and identify the role of an oracle when outside information is needed.
- » Identify possible benefits of transparent, repeatable execution.
- » Evaluate coding, data, upgrade, governance, usability, financial, and legal risks.

KEY TERMS

SMART CONTRACT

Definition: A program deployed at an address on a blockchain. It stores data and carries out defined functions when a transaction or another contract calls those functions.

Sample sentence: The smart contract applied the written rule after an authorized transaction supplied the required input.

DECENTRALIZED APPLICATION

Definition: An application, often called a dapp, that uses one or more smart contracts on a decentralized network and usually includes a user interface and other supporting components.

Sample sentence: The decentralized application gave users a readable screen for requesting an action from the underlying smart contract.

CODE

Definition: Instructions written in a programming language so that a computer can perform defined operations.

Sample sentence: The code checked whether the recorded conditions were satisfied before producing an output.

ORACLE

Definition: A service or system that provides a blockchain application with information from outside the blockchain, such as a price, weather result, or verified event.

Sample sentence: The contract relied on an oracle to receive information that the blockchain could not observe by itself.

AUDIT

Definition: A structured technical review of code, design, or controls intended to identify defects and security weaknesses within a stated scope.

Sample sentence: The audit identified a weakness, but it did not guarantee that every future problem had been found.

VULNERABILITY

Definition: A weakness in code, design, configuration, data, or operations that could cause failure or allow misuse.

Sample sentence: A missing authorization check created a vulnerability that could allow an unapproved action.

MAIN LESSON

A SMART CONTRACT IS A PROGRAM ON A BLOCKCHAIN

A conventional program may run on a company server, personal computer, or telephone. A smart contract runs within a blockchain network's computing environment. Once deployed, it has an address. It can store information, receive calls to its functions, check conditions, update its state, and create records under the network's rules.

On Ethereum and compatible networks, a person normally interacts with a smart contract by submitting a transaction that calls a function. Validators process the transaction. Each participating node follows the same network rules and should reach the same result from the same valid starting state and input. The result may update a balance, record a vote, issue a token, transfer an asset, or reject the request.

The transaction requires a network fee. The fee pays for computation and record-keeping. More complex operations may require more computation than a simple transfer. A failed request may still consume network resources and create a fee even when the intended state change does not occur.

A smart contract does not normally begin an action merely because time passes or an event happens in the world. A transaction, another contract, or an authorized automation service must call the relevant function. The code then evaluates the information available to it.

THINK IN TERMS OF INPUT, RULE, STATE, AND OUTPUT

A beginner can understand smart-contract logic without writing code. Use four questions:

- » Input: What information or request enters the program?
- » Rule: What written conditions and calculations will the program apply?
- » State: What information has the program already recorded?
- » Output: What result will the program record or attempt to produce?

Imagine a simple program for issuing one digital completion badge. The input is a learner identifier and an authorized completion report. The rule says that a badge may be issued only when the completion report is valid and no badge has already been issued for that identifier. The state records whether the identifier already received a badge. The output is either a new badge record or a rejected request.

This model helps a learner locate weaknesses. What if the completion report is wrong? What if two people receive the same identifier? What if the authorized reporter loses control of a signing credential? What if the rules contain no correction process? The program may follow its instructions exactly and still produce an unfair or unintended human result.

“SMART” DOES NOT MEAN INTELLIGENT

A smart contract does not understand purpose, fairness, hardship, or context unless people translate a limited part of those ideas into explicit conditions. It cannot



recognize an exception that the designers failed to include. It does not reconsider a decision because the outcome feels wrong.

The code may be complex, but complexity is not judgment. A program can calculate a fee precisely while applying the wrong fee rate. It can reject an unauthorized request while failing to recognize a newly authorized person. It can produce a consistent result from inaccurate input.

Artificial intelligence and smart contracts are different concepts. Some systems may combine them, but a basic smart contract is not an artificial-intelligence model. It executes programmed logic within the blockchain environment.

“CONTRACT” DOES NOT AUTOMATICALLY MEAN LEGAL AGREEMENT

Some smart contracts help carry out obligations that people have described in a separate agreement. Others create tokens, record votes, operate games, manage access, or perform calculations without serving as a legal contract.

The label does not determine whether an arrangement is legally enforceable. Legal effect may depend on the parties, consent, disclosures, jurisdiction, subject, surrounding documents, and applicable law. Code may perform an action even when people later dispute authority, ownership, fraud, error, or legal responsibility. This course provides education rather than legal advice.

A DECENTRALIZED APPLICATION HAS SEVERAL LAYERS

A decentralized application usually combines a user-facing interface with one or more smart contracts. The interface may be a website, mobile application, or other screen. It helps a person choose an action and prepare a transaction. The smart contract performs the on-chain logic after the request reaches the network.

OTHER COMPONENTS MAY INCLUDE:

- » A wallet or signing tool that authorizes a transaction.
- » A conventional web server that delivers the interface.
- » A data-indexing service that organizes blockchain records for faster display.
- » An oracle that supplies outside information.
- » An administrator or governance process that changes settings or upgrades code.
- » Customer-support, legal, accounting, and operational teams.

These components can have different levels of decentralization. A smart contract may be public while the website is controlled by one company. The contract may be difficult to change while an administrator can change selected settings. The in-



terface may display information from a centralized server. Calling the entire system decentralized does not explain who controls each layer.

When evaluating a dapp, ask who controls the interface, code, administrative keys, upgrades, data sources, treasury, and public communications. Also ask what happens if one component fails.

ORACLES CONNECT CODE WITH OUTSIDE INFORMATION

A blockchain can verify information already available under its own rules. It cannot independently observe the weather, a court decision, a sports result, the value of an off-chain asset, or whether a learner completed a course. An oracle brings selected outside information into the blockchain environment.

The oracle expands what a smart contract can do, but it also creates a new dependency. If the source is wrong, delayed, manipulated, unavailable, or misunderstood, the contract may execute correctly from bad data. Multiple data providers or verification methods can reduce some risks, but they do not turn an uncertain outside event into perfect information.

An oracle also does not decide whether a rule is fair. It reports data according to its design. People remain responsible for choosing sources, resolving disputes, designing correction procedures, and deciding whether automated action is appropriate.

APPLIED CASE: THE INDEPENDENT PP TOKEN COMMUNITY

The independent PP token community provides a real example of smart-contract logic on BNB Smart Chain. The community website clearly states that the token is not an official Prison Professors project or endorsement. Neither CZ nor I created the token, and Prison Professors did not organize, manage, or control the project.

The public community website describes a 3 percent charge on buy or sell trades. It says that the smart contract collects the charge and directs resources toward a public mission wallet. A public BscScan page identifies the PP token contract and displays source information for code containing transaction-fee logic.

We can organize the example with the four-question model:

- » Input: A trade involving the token and the recognized trading pair.
- » Rule: Calculate the programmed fee under the contract's conditions and allocate it according to configured percentages.
- » State: Track balances, fee settings, recorded allocations, and other contract data.
- » Output: Update token balances and process the fee according to the code.

That description is simplified. The actual code contains additional functions, roles, conditions, and dependencies. A public source display can help a qualified reviewer examine the logic. It does not prove that every user understands the code, that the code has no vulnerability, that every website statement is complete, or that every off-chain action will follow a mission.

The case also separates several components that a learner may otherwise combine. The token contract contains on-chain rules. BNB Smart Chain processes transactions. BscScan displays public records and source information. The community website communicates the project's description. A public treasury address shows selected on-chain activity. Prison Professors carries out its educational mission through people, policies, institutions, and programs outside the contract.

Future lessons will use this same case to examine decentralized finance and governance. The purpose is education. No participant is being asked to acquire the token, visit the website, connect a wallet, approve a contract, or conduct a transaction.

TRANSPARENT AND REPEATABLE EXECUTION CAN OFFER BENEFITS

Smart contracts can support useful designs when the rules are suitable for automation.

- » The same valid input can produce the same result under the same recorded state.
- » Public code and transaction records may allow independent inspection.
- » Automated calculations can reduce some manual steps and delays.
- » Shared rules can coordinate people or organizations that use the same network.
- » One contract may interact with another, allowing developers to combine existing components.
- » Records can show when a function was called and what on-chain result followed.

These benefits are conditional. Public code helps only when someone can understand it. Repeatability reproduces a defect as consistently as it reproduces a correct rule. Composability can spread a failure from one component into another. Automation can reduce one human bottleneck while creating a different dependency.

CODING AND DESIGN RISKS

Code is written by people. Developers can misunderstand a requirement, omit a condition, use an unsafe pattern, or connect components incorrectly. Common classes of smart-contract weakness include broken access controls, faulty business

logic, unvalidated inputs, unsafe external calls, calculation errors, oracle manipulation, and upgrade problems.

A small defect can have a large effect when code controls valuable assets or a widely used application. Public deployment may allow many people and other contracts to interact with the same weakness before maintainers can respond.

Testing and review reduce risk but cannot prove perfection. A contract may behave correctly during expected tests and fail under an unusual sequence of actions. A dependency may change. A new interaction may expose a weakness that was not included in the original review.

UPGRADE AND GOVERNANCE RISKS

Some contracts are designed to be difficult or impossible to change. That can protect users from unexpected changes, but it can also preserve defects. Other systems use upgrade mechanisms or administrative settings. Those features can support repairs, but they give selected people or governance processes power over future behavior.

ASK:

- » Can the code be upgraded or replaced?
- » Who can change settings, fees, permissions, or destinations?
- » Is a delay, vote, or multiple-signature approval required?
- » Can users observe a proposed change before it takes effect?
- » What happens if an administrator loses a key or abuses authority?

The word decentralized does not answer these questions. Control may be distributed in one part of the system and concentrated in another.

INTERFACE AND USABILITY RISKS

Most users do not read source code. They rely on an interface that translates a human choice into transaction data. A confusing or dishonest interface can describe one action while preparing another. A copied website can imitate a legitimate application. A wallet screen may display technical permissions that a beginner cannot interpret.

The underlying contract can also be genuine while the user selects the wrong network, address, function, or amount. Technical validity does not establish that the action matches the user's purpose.

No learner should connect to an application merely to understand this lesson. Paper analysis can build the same foundational judgment: identify the components, locate the decision points, and ask what evidence supports each claim.

FINANCIAL, OPERATIONAL, AND LEGAL RISKS

Smart-contract use may involve transaction fees, changing asset values, limited liquidity, network congestion, irreversible errors, and dependence on other contracts. An application may fail even when its own code works because an oracle, interface, administrator, market, network, or external institution fails.

Legal and operational responsibilities also continue. A public record does not automatically establish identity, lawful authority, ownership, compliance, accounting treatment, tax treatment, consumer protection, or enforceability. Organizations still need human policies for authorization, custody, records, privacy, dispute handling, and accountability.

AN AUDIT IS EVIDENCE, NOT A GUARANTEE

An audit can identify weaknesses within the code version, assumptions, and scope reviewed. A useful audit report should allow a reader to understand what was examined, when the review occurred, which findings were identified, and whether reported changes were rechecked.

An audit does not guarantee that the code is free from defects. It may exclude the website, oracle, governance process, administrative keys, later upgrades, or connected contracts. A logo stating “audited” is not enough to evaluate scope or quality.

The same disciplined approach applies here as in earlier lessons: separate a claim from the evidence supporting it. Ask what the evidence shows, what it leaves unresolved, and what could change after the review.

HUMAN JUDGMENT REMAINS PART OF THE SYSTEM

Smart contracts can automate narrow rules. People still decide which problem to address, which rules to write, which data to trust, who can change the system, how to communicate risks, and how to respond when the output harms someone.

Good design does not try to automate every decision. It identifies where consistency helps and where discretion, appeal, investigation, or compassion is required. A correction process may be as valuable as the original rule.

Self-directed learning works in a similar way. A study schedule can create structure, but the schedule cannot judge whether you understood the lesson. You must review your work, identify gaps, seek feedback, and adjust. Code can support a process. It cannot replace the person responsible for the outcome.

APPLIED SCENARIO: THE COMPLETION BADGE DISPUTE

The following scenario is fictional and requires no device or account.

An education organization creates a dapp that issues digital course-completion badges. An approved educator sends a completion result to an oracle. The oracle places that result on the blockchain. A smart contract then issues one badge to the learner identifier when all recorded conditions are satisfied.

THE CODE CHECKS FOUR ITEMS:

- » The report came through the approved oracle.
- » The report says “completed.”
- » The learner identifier has not received a badge before.
- » The request arrived before the program deadline.

A learner completed the course, but the educator accidentally submitted “not completed.” The oracle accurately delivered that incorrect report. The smart contract rejected the badge request. The program contains no appeal, correction, pause, or replacement process.

The code followed its instructions. The oracle delivered the data it received. The human result was still wrong.

Use the scenario to separate responsibilities:

- » The educator created the original information.
- » The oracle transported the information into the blockchain environment.
- » The smart contract applied the written conditions.
- » The dapp interface displayed the result.
- » The organization designed the policy and omitted a correction path.

The organization should not describe the result as correct merely because the code executed successfully. A better design could include a documented review process, correction authority, time delay, second source, or appeal before a permanent badge record is issued.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Defined rules can execute consistently across valid requests.
- » Public records may support inspection of selected actions and results.
- » Automation can reduce some repetitive manual work.

- » Shared code can coordinate participants across organizations.
- » Smart contracts can interact with other contracts to build larger systems.
- » A clear input–rule–output model can improve process design even when a blockchain is not used.

LIMITATIONS AND RISKS

- » Code can contain vulnerabilities, missing conditions, and misunderstood requirements.
- » Correct code can produce a harmful result from inaccurate or manipulated data.
- » Oracles introduce outside sources, operators, availability needs, and trust assumptions.
- » Upgrade rights and administrative settings can concentrate power.
- » Immutable code can preserve a defect, while upgradeable code creates change-control risk.
- » Interfaces may be centralized, misleading, unavailable, or compromised.
- » Users may not understand the permissions or transaction data presented to them.
- » Network fees, congestion, market conditions, and connected contracts can alter practical outcomes.
- » Audits have a scope and date; they do not guarantee future safety.
- » On-chain execution does not resolve every legal, ethical, accounting, privacy, or governance question.

COMMON MISCONCEPTIONS

“Smart contracts think.” They execute programmed logic. They do not understand intent, fairness, or context.

“Every smart contract is a legal contract.” Some code supports an agreement, while other code manages tokens, votes, games, or records. Legal effect depends on facts and applicable law.

“Code removes trust.” A system may shift trust toward developers, administrators, oracle operators, interface providers, auditors, governance participants, or data sources.

“A successful transaction proves a good outcome.” The network may process the instructions correctly even when the input was wrong or the human purpose was not achieved.

“A dapp is decentralized in every component.” The smart contract may be public while the website, data service, administrator, or communication channel remains centrally controlled.

“An audit proves the contract is safe.” An audit is a bounded review. Defects, excluded components, later changes, or new interactions may remain.

“Public code is easy for everyone to verify.” Availability is not the same as understanding. Skilled review, documentation, and clear communication remain necessary.

“Automation eliminates governance.” People still set rules, assign authority, approve upgrades, select data sources, and respond to failures.

OFFLINE EXERCISE: TEST THE MISSING CONDITION

Estimated time: 25–30 minutes

Materials: Separate paper and a pencil.

You will simulate a fictional smart contract for a learning-credit program. The credits have no cash value and exist only for this exercise.

The paper program has four inputs:

- » Participant code
- » Completion report: completed or not completed
- » Report source: authorized or unauthorized
- » Previous credit recorded: yes or no

Apply these written rules in order:

1. If the report source is unauthorized, write REJECT.
2. If the report says not completed, write REJECT.
3. If a previous credit is recorded, write REJECT.
4. If the source is authorized, the report says completed, and no previous credit exists, write APPROVE ONE CREDIT.

Test the rules against four cases:

CASE A: EXPECTED APPROVAL

Participant code P-101 has an authorized completion report and no previous credit. Record the output and identify the rule that produced it.



CASE B: UNAUTHORIZED SOURCE

Participant code P-102 has a completed report from an unauthorized source and no previous credit. Record the output and explain why the claimed completion alone is insufficient.

CASE C: INCORRECT INPUT

Participant code P-103 completed the course, but an authorized source mistakenly reports not completed. Record the output required by the code. Then explain why correct execution produced an incorrect human result.

CASE D: DUPLICATE IDENTIFIER

Two participants were mistakenly assigned code P-104. The first participant received a credit. The second participant later submits an authorized completion report under the same code. Record the output and explain the identity problem.

After completing all four cases, answer these questions:

- » Which inputs came from people or outside systems?
- » Which outputs followed the written rules correctly?
- » What correction, appeal, or identity condition did the designers omit?
- » What role could a second reviewer play before the output becomes permanent?
- » Would every part of this process benefit from automatic execution? Explain your answer.
- » Write one revised rule that improves the process without claiming to solve every possible error.

The exercise simplifies real smart-contract development. Actual code requires programming, testing, security review, network deployment, and operational controls. The purpose here is to practice identifying assumptions and missing conditions.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes a smart contract?
 - a. An intelligent system that can judge fairness and intent
 - b. Code deployed on a blockchain that carries out defined functions when called
 - c. A legal agreement that is automatically enforceable in every jurisdiction



- d. A customer-service process that can reverse every transaction
- 2. Which description best fits a decentralized application?
 - a. A smart contract with no interface, supporting service, or human control
 - b. Any website that uses the word blockchain
 - c. An application that uses smart contracts on a decentralized network and may also rely on interfaces, wallets, data services, or administrators
 - d. A program that cannot contain centralized components
- 3. Why might a smart contract use an oracle?
 - a. To obtain selected information from outside the blockchain
 - b. To guarantee that all outside information is true
 - c. To replace every human decision with artificial intelligence
 - d. To eliminate the need for a transaction or function call

TRUE OR FALSE

- » A completed audit guarantees that a smart contract, its interface, its data sources, and all future upgrades are free from vulnerabilities.

SHORT EXPLANATION

- » In four or five sentences, use the independent PP token community case or the completion-badge scenario to explain one action code can automate and two forms of human judgment or accountability that code does not replace.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A smart contract is code deployed at a blockchain address.
- » A transaction, another contract, or an authorized service normally triggers a function.
- » Inputs, rules, stored state, and outputs provide a useful model for analyzing the code.
- » A smart contract is not automatically intelligent or legally enforceable.
- » A dapp usually combines smart contracts with an interface and other supporting components.
- » Different parts of a dapp can have different levels of decentralization and control.
- » An oracle supplies selected outside information that a blockchain cannot observe by itself.
- » Correct code can produce an unintended result when the input or rule is wrong.



- » Public source information can support inspection without guaranteeing safety or complete understanding.
- » Audits can identify weaknesses within a defined scope and time; they cannot prove perfection.
- » Upgradeability supports correction but creates authority and governance risks.
- » Immutable code limits changes but can preserve defects.
- » Interfaces, administrators, data sources, connected contracts, and human policies remain part of the system.
- » The independent PP token community shows how code can apply fee logic while people remain responsible for mission, governance, communication, and use of resources.
- » No course activity requires a wallet, asset, application connection, programming, or transaction.

The practical takeaway is direct: evaluate both the automated rule and the human system surrounding it. Ask what the code can do, what information it depends on, who can change it, and what happens when the output is wrong.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a clear explanation:

- » Define a smart contract and decentralized application in your own words.
- » Explain one task that code can perform consistently.
- » Explain why correct execution does not guarantee a fair, safe, legal, or useful human outcome.
- » Use the independent PP token community case or the completion-badge scenario to identify the input, rule, state, and output.
- » Describe one missing condition or inaccurate input that could create a harmful result.
- » Explain the role of an oracle and one risk that accompanies outside data.
- » Describe what an audit can show and what it cannot guarantee.
- » Identify one decision that should remain subject to human review, appeal, or accountability.



- » Connect the lesson to your own self-directed learning. Explain how written routines can support your progress without replacing reflection, feedback, and adjustment.

Your response should demonstrate technical understanding, critical thinking, and personal responsibility. Do not visit a website, connect a wallet, create an account, write deployable code, acquire an asset, or perform a transaction. Do not include any real password, private key, seed phrase, authentication code, wallet address, balance, transaction identifier, or financial-account information.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 16: Smart Contracts and Decentralized Applications, and the date you completed the entry.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 16 — [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 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 identifiers, transaction details, or other sensitive information in a Profile response.

UNDERSTANDING WEB3**LESSON 17: DECENTRALIZED FINANCE**

A Prison Professors Self-Directed Course

Estimated time: 75–110 minutes

Educational and Safety Boundary:

This lesson provides general education about decentralized finance and related risks. It does not provide individualized financial, investment, legal, or tax advice. No activity requires internet access, an account, a wallet, a digital asset, or a transaction.

OPENING GUIDANCE

While serving 26 years in federal prison, I learned to pause when a promise sounded unusually attractive. I could not afford to build my future around a slogan. I had to ask where an opportunity came from, what work it required, who controlled it, what could fail, and what evidence supported the claim.

That habit applies directly to decentralized finance, often shortened to DeFi. A person may encounter phrases such as earn yield, instant liquidity, permissionless exchange, or automatic lending. Those phrases describe possible features. They do not establish safety, reliability, legality, fairness, or a guaranteed return.

DeFi uses blockchains, tokens, smart contracts, wallets, interfaces, and outside data to provide financial-like functions. Those functions can include exchanging one token for another, supplying assets to a pool, borrowing against collateral, and distributing fees or incentives. The code can automate calculations and transfers. People still design the system, choose its rules, supply its assets, control selected settings, communicate its claims, and absorb its losses.

I encourage you to approach this lesson as a systems analyst rather than as a customer. You do not need money, internet access, or a wallet. Your task is to trace how a proposed service works and identify the conditions behind any advertised benefit.

The independent PP token community will provide one practical example. Neither Prison Professors nor I created, organized, managed, or controlled that token project. Community members formed it as an independent effort. A public page displays a trading pair between the PP token and Wrapped BNB on BNB Smart Chain. That pair helps us see how a decentralized exchange can use a liquidity pool. It does not ask or encourage anyone to acquire or trade the token.

Keep one question in view: If someone describes a possible return, what risks, dependencies, and loss pathways should I examine before accepting the claim?

PURPOSE AND ESSENTIAL QUESTION

Lesson 17 introduces blockchain-based exchanges, lending, borrowing, and liquidity without encouraging participation or minimizing risk. It explains how smart contracts may coordinate these functions and why DeFi can retain important forms of human control and financial exposure.

Essential Question:

- » Why should a promise of greater return lead to more questions about risk, liquidity, control, and possible loss?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define decentralized finance at an introductory level.
- » Describe the basic functions of decentralized exchanges, lending protocols, and liquidity pools.
- » Explain the possible roles of collateral and automated pricing.
- » Identify smart-contract, liquidation, liquidity, volatility, oracle, governance, fraud, and regulatory risks.

KEY TERMS

DECENTRALIZED FINANCE

Definition: A broad term for blockchain-based services that use smart contracts to perform financial-like functions such as exchanging, lending, borrowing, or distributing returns, often without a conventional institution handling every step.

Sample sentence: The decentralized finance protocol used smart contracts to coordinate a pool of tokens, but people still governed important settings.

DECENTRALIZED EXCHANGE

Definition: A blockchain-based protocol, often called a DEX, that allows token exchanges through smart contracts rather than relying only on a conventional exchange to hold assets and update an internal account ledger.

Sample sentence: The decentralized exchange used a liquidity pool to calculate the terms of a token swap.

LIQUIDITY POOL

Definition: Tokens placed in a smart contract so that the protocol can support exchanges, loans, or other functions.

Sample sentence: The liquidity pool needed enough available tokens to support the requested exchange.

COLLATERAL

Definition: An asset pledged to support an obligation and exposed to being taken or sold if the required conditions are not maintained.

Sample sentence: The borrower pledged a volatile token as collateral for a smaller loan.

LIQUIDATION

Definition: A process that sells or transfers collateral after a borrowing position crosses a defined risk threshold.

Sample sentence: A rapid decline in the collateral's value caused the smart contract to make the position eligible for liquidation.

YIELD

Definition: A return associated with providing, lending, staking, or otherwise committing an asset. Yield may come from interest, trading fees, token incentives, or another source, and it is not guaranteed profit.

Sample sentence: Before evaluating the advertised yield, the learner identified its source, conditions, and possible paths to loss.

MAIN LESSON

DEFI DESCRIBES FUNCTIONS, NOT A SINGLE PRODUCT

DeFi is not one company, application, blockchain, or legal structure. It is a broad category. Different protocols use different code, assets, governance arrangements, data sources, interfaces, and risk controls.

A DeFi system may attempt to perform functions that also exist in conventional finance:

- » Exchange one asset for another.
- » Match people who supply assets with people who borrow.

- » Require collateral to support a loan.
- » Calculate interest or other charges.
- » Distribute trading fees or token incentives.
- » Create derivatives, insurance-like arrangements, or asset-management tools.

The financial function may be familiar even when the delivery system is new. A borrower still faces an obligation. A lender still faces the possibility of loss. A market still needs buyers, sellers, and usable liquidity. Prices can still move. Fraud can still occur. The new features include programmable execution, public blockchain records, token-based assets, and the ability to combine one protocol with another.

The word decentralized should be treated as a question, not a complete description. A system may distribute transaction processing across a blockchain while concentrating control over its website, administrative keys, upgrades, oracle selection, treasury, or governance tokens.

A DEFI SERVICE HAS SEVERAL CONNECTED LAYERS

Lesson 16 introduced the layers of a decentralized application. DeFi builds financial exposure on top of those layers. A simple DeFi service may depend on:

- » A blockchain that processes transactions and stores the current state.
- » Tokens that represent the assets used by the protocol.
- » Smart contracts that hold assets and apply rules.
- » A wallet or signing tool that authorizes requests.
- » A website or other interface that prepares those requests.
- » Oracles that supply prices or other outside information.
- » Liquidity providers who place assets into pools.
- » Governance participants or administrators who set or change parameters.
- » Bridges, stablecoin issuers, custodians, or other connected services.

A failure in one layer can affect the rest. Correct smart-contract code cannot repair an inaccurate oracle price. A public blockchain cannot guarantee that a stablecoin issuer can honor redemptions. A well-designed protocol cannot prevent every copied website from imitating its interface. An available pool cannot protect a participant from a sharp change in token value.

This layered view also prevents a common misunderstanding: removing one conventional intermediary does not remove every dependency. DeFi often rearranges trust. A participant may rely less on a bank's internal ledger and more on code, collateral, market liquidity, token issuers, oracle operators, governance, and personal security.

DECENTRALIZED EXCHANGES

A decentralized exchange uses smart contracts to support token exchanges on a blockchain. In many designs, a participant keeps control of assets until a signed transaction interacts with the protocol. The protocol then applies its rules and updates on-chain balances.

This differs from a centralized exchange that commonly receives a customer's assets, holds them in accounts under the company's control, and records many trades on an internal ledger. A DEX can reduce reliance on that form of custody, but it creates other exposures:

- » A person must protect the credentials used to authorize a transaction.
- » The smart contract may contain a defect or unsafe feature.
- » A copied interface may prepare a harmful request.
- » A token may be fraudulent, restricted, illiquid, or controlled by an unknown party.
- » A transaction can fail, execute at an unexpected price, or incur fees.
- » The protocol may rely on governance or administrative powers.
- » Laws and access restrictions may apply even when code is publicly reachable.

Some decentralized exchanges match orders. Others use an automated market maker. The next section explains that model.

LIQUIDITY POOLS AND AUTOMATED PRICING

An automated market maker, often shortened to AMM, uses a formula and a pool of tokens to quote exchanges. Instead of waiting for a specific seller to accept a specific buyer's order, a trader exchanges against assets already held by a smart contract.

Imagine a pool that contains Token A and Token B. The protocol observes the pool's balances and applies a pricing formula. When a person sends Token A into the pool and receives Token B, the balance of Token A rises while the balance of Token B falls. The formula produces a new exchange rate after the trade.

This is automated pricing. It does not mean the protocol knows the fair economic value of either token. The formula responds to pool balances. Traders, arbitrage activity, outside markets, and available liquidity influence how the pool's price relates to prices elsewhere.

Trade size can influence the result. A small trade in a deep pool may change the balance only slightly. A large trade in a shallow pool may move the quoted price

more sharply. The difference between an expected price and the execution result is commonly called slippage.

Liquidity providers supply the pool's tokens. In return, the protocol may allocate a share of trading fees or other incentives. That possible return carries exposure:

- » One or both tokens can lose value.
- » Pool prices can change rapidly.
- » A provider's final mix of tokens can differ from the starting mix.
- » The provider may perform worse than simply holding the original tokens.
- » Smart-contract defects, governance changes, scams, or network failures can cause loss.
- » A withdrawal may be difficult when liquidity is limited or the system is paused.

The phrase impermanent loss is often used for the difference that can arise when the relative prices of pooled tokens change and the automated market maker rebalances the provider's holdings through trades. The label can mislead beginners. The loss does not necessarily disappear. If a person withdraws under unfavorable conditions, the economic difference can become final.

APPLIED CASE: THE INDEPENDENT PP TOKEN PAIR

The independent PP token community provides a real example of a token pair on BNB Smart Chain. Neither CZ nor I created the token. Prison Professors did not organize, manage, or control the project, and the community describes it as independent rather than as an official Prison Professors product or endorsement.

On July 23, 2026, a public DEX Screener page identified a PP/WBNB pair on PancakeSwap v2. WBNB means Wrapped BNB, a token form of BNB that can interact consistently with smart contracts. The page displayed two assets pooled in a smart contract and identified a public pair address.

That observation gives us a five-part map:

- » Asset one: the community-created PP token.
- » Asset two: WBNB.
- » Pool: a smart contract holding quantities of both assets.
- » Pricing process: an automated market-maker formula that changes the pool's exchange rate as trades alter its balances.
- » Interface and record tools: PancakeSwap may prepare interactions, while DEX Screener and BscScan display selected public information.

The pair illustrates a basic DeFi function. It does not prove that either token has a stable value, that the pool will remain liquid, that every contract is safe, that displayed information is complete, or that a trade will produce a favorable result. A listing is not an endorsement, and a public record is not a recommendation.

The community token also has its own smart-contract behavior and public mission claims. Those features are separate from the DEX pool's pricing and liquidity. A learner should identify which contract performs which function instead of treating the token, pair, website, treasury, and Prison Professors organization as one system.

No participant should visit the page, connect a wallet, approve a contract, acquire a token, or conduct a trade for this course. The educational value comes from tracing the system on paper.

LENDING AND BORROWING PROTOCOLS

A DeFi lending protocol may gather tokens from suppliers into a pool. Borrowers receive tokens from that pool after satisfying the protocol's conditions. Smart contracts track supplied assets, borrowed assets, interest, collateral values, and risk thresholds.

The word lender can create the image of one person evaluating another person's character and repayment history. Many DeFi protocols use a different model. Suppliers contribute to a shared pool. Borrowers interact with the pool's rules. The protocol may not know the borrower's identity or credit history. It instead relies heavily on collateral.

Interest rates may change according to pool use and governance settings. When much of an available pool has been borrowed, the protocol may increase borrowing rates to encourage repayment and attract more supply. When demand is lower, rates may decline. A displayed rate can therefore change rather than remain fixed.

Available liquidity affects withdrawals. A supplier's account may show a claim on the pool while much of the underlying asset is currently borrowed. The protocol may allow withdrawal only when enough unborrowed liquidity is available. The phrase withdraw anytime should be examined together with the conditions that can limit actual withdrawal.

COLLATERAL AND OVERCOLLATERALIZATION

Collateral reduces one form of lending risk by giving the protocol an asset that can be taken or sold if the borrowing position becomes unsafe. Many crypto lending designs require overcollateralization: the collateral must be worth more than the borrowed amount when the loan begins.



Suppose a fictional protocol requires \$150 of Token A as collateral for a \$100 loan of Token B. The extra value creates a buffer. If Token A's market value falls, that buffer shrinks. If the value crosses the protocol's threshold, the position may become eligible for liquidation.

Overcollateralization does not remove risk. It moves much of the risk toward:

- » The accuracy and timeliness of price data.
- » The speed and depth of markets used to sell collateral.
- » The volatility of the pledged token.
- » The reliability of the liquidation code.
- » Network availability and transaction ordering.
- » The borrower's ability to monitor a changing position.
- » Governance decisions about thresholds, accepted assets, and fees.

A protocol may permit a person to borrow without a conventional credit check, but that person can still lose valuable collateral. Privacy or access benefits should not be separated from the economic cost of maintaining the position.

LIQUIDATION IS AN AUTOMATED LOSS-CONTROL PROCESS

Liquidation is the process used to restore a protocol's collateral protection after a borrowing position crosses a defined threshold. A smart contract may allow another participant or automated service to repay part of the debt and receive part of the collateral, often with an incentive.

From the protocol's perspective, liquidation can reduce the chance that a loan becomes undercollateralized. From the borrower's perspective, liquidation can cause an involuntary sale or transfer of collateral, a penalty, and a realized loss.

Rapid markets can make the process severe. A falling collateral price can trigger many liquidations. Those sales can place further pressure on market prices. Thin liquidity, oracle delays, network congestion, or aggressive thresholds can worsen the result.

The code may perform the authorized liquidation exactly as designed. The outcome can still be financially painful. Automation increases speed and consistency; it does not create compassion, negotiation, an extension, or a guaranteed opportunity to recover.

ORACLES CAN DETERMINE FINANCIAL OUTCOMES

A blockchain cannot independently know the current market value of an asset. A lending protocol may use an oracle to obtain price information. The reported price

helps calculate collateral value and decide whether a position has crossed a liquidation threshold.

That dependency creates several questions:

- » Which markets or data providers contribute to the price?
- » How often does the value update?
- » What happens when a source is unavailable?
- » Can one market be manipulated?
- » Does the protocol compare several sources?
- » Is there a delay, pause, or review mechanism for an extreme result?
- » Who can replace or reconfigure the oracle?

An oracle can transmit data correctly according to its design while the data remains incomplete, delayed, or distorted. If a protocol uses that value automatically, a data weakness can become a financial loss.

YIELD HAS A SOURCE AND A SET OF CONDITIONS

Yield does not appear from nowhere. A protocol may distribute value from:

- » Interest paid by borrowers.
- » Fees paid by traders.
- » Newly issued incentive tokens.
- » Rewards funded by a project treasury.
- » Revenue from another strategy or connected protocol.
- » Subsidies intended to attract early participation.

Each source creates different questions. Borrower interest depends on borrowers, collateral, repayment, and available liquidity. Trading fees depend on trading activity and pool design. Incentive tokens depend on the token's supply, demand, transferability, governance, and market value. A connected strategy adds another contract and another path to failure.

An advertised percentage may be variable, estimated, annualized from a short period, paid in a volatile token, reduced by fees, or dependent on reinvestment. The number may describe a gross rate before token-price losses, taxes, withdrawal costs, or liquidation.

Greater advertised yield commonly reflects greater uncertainty, risk, or subsidy. It should produce a longer list of questions:



- » What creates the return?
- » Who pays it?
- » In which asset is it paid?
- » Can that asset lose value?
- » Is the rate fixed, variable, promotional, or estimated?
- » Can principal be lost?
- » Can assets be withdrawn when requested?
- » Which contracts, oracles, bridges, administrators, and markets are involved?
- » What evidence supports the claim?
- » What legal protections or remedies exist if the system fails?

The purpose of these questions is not to predict every failure. It is to replace excitement with analysis.

SMART-CONTRACT AND COMPOSABILITY RISK

DeFi protocols can connect to other protocols. One application may deposit assets into a second protocol, use a token from that protocol as collateral in a third, and rely on an oracle drawing data from several markets. This ability to combine components is called composability.

Composability can support new services without rebuilding every function. It also connects risks. A defect, pause, price failure, governance attack, or liquidity shortage in one component can spread into another.

An audit can provide useful evidence about a defined code version and scope. It cannot guarantee the safety of connected contracts, later upgrades, user interfaces, governance decisions, oracle data, bridges, or market conditions. A high yield should not be treated as compensation for risks that the participant cannot identify or evaluate.

LIQUIDITY AND VOLATILITY RISK

Liquidity is the practical ability to exchange or withdraw an asset without unacceptable delay or price impact. A displayed balance does not prove that a market can absorb a large sale. A pool can exist while remaining too shallow for the desired transaction.

Volatility can reduce collateral values, trigger liquidation, change pool composition, and overwhelm price assumptions. A token advertised as stable may lose its intended reference value. A wrapped token may depend on a custodian or contract. A bridge may fail. Each additional token representation adds a dependency.



Liquidity can disappear during stress, precisely when many people want to exit. Transaction fees and network congestion may rise at the same time. A participant may face both a falling price and difficulty completing a protective action.

GOVERNANCE AND ADMINISTRATIVE RISK

Some protocols use token voting. Others rely on a development team, foundation, company, multisignature group, or administrator. Many use a combination.

Governance or administrators may be able to:

- » Change collateral requirements or interest-rate formulas.
- » Add or remove supported assets.
- » Select or replace oracles.
- » Pause functions.
- » Upgrade contracts.
- » Redirect fees.
- » Control a treasury.
- » Influence the interface and public communications.

These powers can support repairs and adaptation. They can also concentrate control or create misuse, key-loss, and conflict-of-interest risks. A protocol can process transactions on a decentralized network while important decisions remain concentrated among a small group.

FRAUD, MANIPULATION, AND LEGAL UNCERTAINTY

Open code and public networks do not prevent deception. A promoter may copy a known protocol's website, invent an audit, conceal administrator powers, create a token with harmful transfer rules, exaggerate a yield, or disappear after collecting assets.

Market manipulation can distort prices in shallow pools. An attacker may exploit code, governance, an oracle, a bridge, or transaction ordering. Recovery may be difficult because blockchain transactions can be irreversible and participants may be unknown or located across jurisdictions.

Legal and regulatory treatment varies by activity, asset, participant, and jurisdiction. Public availability does not establish legal permission. Terms such as decentralized, community-owned, or autonomous do not remove possible obligations or liability. This course does not provide legal advice.

A DISCIPLINED EVALUATION SEQUENCE

When you examine a DeFi claim on paper, use this sequence:

PRISON PROFESSORS CHARITABLE CORPORATION



1. Identify the function. Is it exchange, lending, borrowing, liquidity provision, or something else?
2. Identify the assets. What tokens enter, leave, secure, or pay the arrangement?
3. Identify the source of return. Interest, trading fees, incentives, treasury subsidy, or another strategy?
4. Identify the controls. Who can upgrade, pause, change rates, choose oracles, or move resources?
5. Identify the loss pathways. Price decline, liquidation, code defect, fraud, illiquidity, bridge failure, or governance action?
6. Identify the exit conditions. When and how can a participant withdraw, and what can delay or reduce the result?
7. Identify the evidence. Which claims are supported by public records, code, reports, policies, or independent review?
8. Identify the unknowns. Which conditions cannot be verified or understood?

A learner can apply this sequence to financial claims, business opportunities, educational programs, and career pathways. Strong judgment begins with a clear map of how a claimed benefit is produced.

APPLIED SCENARIO: THE RIVERBRIDGE YIELD CLAIM

The following scenario is fictional and requires no device, account, or asset.

RiverBridge describes itself as a decentralized lending application. Its printed advertisement says:

“Earn up to 18 percent annual yield on StudyDollar deposits. Withdraw whenever you choose. Smart contracts remove the middleman.”

The accompanying description provides these details:

- » Depositors supply StudyDollar tokens to a lending pool.
- » Borrowers pledge RiverToken as collateral and receive StudyDollar loans.
- » An oracle reports the market price of RiverToken.
- » The protocol can liquidate collateral when its value crosses a set threshold.
- » The advertised yield includes borrower interest and newly issued RIVER reward tokens.
- » The rate changes with borrowing demand and the market value of RIVER.
- » Withdrawals depend on StudyDollar remaining available in the pool.
- » An administrator can pause withdrawals and upgrade selected contracts.



- » StudyDollar is issued by a separate organization.
- » No independent audit report or legal disclosure accompanies the advertisement.

The advertisement contains a possible return, but the supporting conditions create several forms of exposure.

If RiverToken falls rapidly, borrower collateral may lose value. Liquidations may add selling pressure. If the oracle is delayed or manipulated, the protocol may liquidate at a distorted price or fail to act in time. If most StudyDollar tokens have been borrowed, depositors may have to wait for available liquidity. If RIVER reward tokens lose value, the advertised yield may be worth far less than the displayed percentage suggests.

The administrator's pause and upgrade powers may help respond to a defect, yet those same powers create dependence on a person or group. The separate StudyDollar issuer adds another layer. A smart contract cannot guarantee that the issuer will maintain the token's intended value.

The phrase up to 18 percent is incomplete without a time period, calculation method, payment asset, fees, assumptions, and loss disclosure. The phrase withdraw whenever you choose conflicts with the statement that withdrawals depend on available pool liquidity and may be paused.

The scenario does not prove that RiverBridge is fraudulent. It shows why a short promotional claim is not enough to evaluate a complex financial system.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Smart contracts can automate exchanges, interest calculations, collateral checks, and distributions.
- » Public blockchain records may allow selected transactions, balances, and contract activity to be inspected.
- » A person may retain control of assets until authorizing a protocol interaction.
- » Shared liquidity pools can coordinate assets supplied by many participants.
- » Open protocols can support applications built by different developers.
- » Paper analysis of DeFi can strengthen financial literacy, systems thinking, and risk evaluation.

LIMITATIONS AND RISKS

- » Code can contain defects, hidden permissions, unsafe upgrades, or misunderstood rules.



- » An interface can be copied, compromised, misleading, or unavailable.
- » Oracles can report delayed, incomplete, manipulated, or unsuitable data.
- » Collateral can lose value and trigger automatic liquidation.
- » A liquidity pool can be too shallow to support an expected exchange or withdrawal.
- » Yield can fall, be paid in a volatile token, or fail to compensate for principal loss.
- » Smart-contract composition can carry a failure from one protocol into another.
- » Stablecoins, wrapped assets, bridges, and custodians add dependencies.
- » Governance tokens or administrative keys can concentrate control.
- » Public transactions can expose financial activity without identifying every participant accurately.
- » Fraud and market manipulation can operate through public networks.
- » Legal obligations and available remedies vary across jurisdictions and facts.

COMMON MISCONCEPTIONS

- » “Decentralized means nobody controls anything.” Control can remain concentrated in upgrades, governance, websites, oracles, treasuries, and administrative keys.
- » “A DEX has no intermediaries.” A DEX can reduce reliance on a conventional custodian while adding reliance on code, liquidity providers, interfaces, networks, and governance.
- » “A formula discovers the true price.” An automated market maker calculates a pool price from its rules and balances. It does not know an asset’s fair value.
- » “Liquidity shown on a screen guarantees an easy exit.” Liquidity can be shallow, change quickly, or become unavailable during stress.
- » “Collateral makes lending safe.” Collateral can fall in value, and liquidation can fail or cause loss.
- » “Liquidation is the same as repayment.” Liquidation is an enforced process that can transfer or sell collateral after a threshold is crossed.
- » “Yield is guaranteed profit.” Yield may be variable, promotional, paid in a volatile token, or outweighed by loss.
- » “An audit removes smart-contract risk.” An audit is limited by its scope, date, assumptions, and reviewed code.



- » “Public records prevent fraud.” Public records provide evidence about selected on-chain activity. They do not prove identity, honesty, lawful conduct, or complete disclosure.
- » “Permissionless access removes legal duties.” Applicable duties can continue even when a protocol is reachable through public code.

OFFLINE EXERCISE: QUESTION THE HIGH-YIELD CLAIM

Estimated time: 30–35 minutes

Materials: Separate paper and a pencil.

Use the fictional RiverBridge scenario. Do not use a website, account, wallet, or real asset.

1. Copy the advertisement’s two central promises: the possible annual yield and the claimed withdrawal access.
2. Identify every stated source of the possible yield.
3. For borrower interest, describe who pays and which conditions allow the payment to continue.
4. For RIVER incentives, explain how a falling token price could reduce the value of the advertised return.
5. Identify the collateral and explain what can cause liquidation.
6. Identify the oracle’s role and one way inaccurate or delayed data could cause loss.
7. Explain why a displayed StudyDollar balance does not prove that enough StudyDollar is available for immediate withdrawal.
8. Identify the administrator’s powers. Write one possible benefit and one possible risk created by those powers.
9. Identify the separate StudyDollar issuer as an additional dependency.
10. List four possible loss pathways for a depositor and four possible loss pathways for a borrower.
11. Write five questions that the advertisement should answer before a reader could evaluate the 18 percent figure.
12. Rewrite the advertisement in two or three sentences so that it communicates both the possible return and the principal risks without using promotional language.

Finish with a paragraph of five to seven sentences:



Why should a promise of greater return produce more questions rather than greater confidence? Connect your answer to the source of return, the possibility of principal loss, withdrawal conditions, and human control.

The exercise does not ask you to decide whether to participate. It asks you to identify how the system works and what information a responsible decision would require.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which description best defines decentralized finance?
 - a. A guarantee that financial activity can occur without risk or human control
 - b. Blockchain-based services that use smart contracts to perform financial-like functions
 - c. Any digital payment processed by a bank
 - d. A legal category that applies identically in every jurisdiction
2. What is the main role of a liquidity pool in an automated market maker?
 - a. It guarantees that both pooled tokens will keep a stable value
 - b. It holds tokens that the smart contract uses to support exchanges under a pricing formula
 - c. It reverses trades when a participant changes direction
 - d. It determines the lawful value of every token
3. Why may a DeFi borrower face liquidation?
 - a. The pledged collateral falls below the protocol's required threshold
 - b. The borrower asks a question about the interest rate
 - c. A block explorer displays the loan
 - d. The borrower keeps more collateral than the protocol requires

TRUE OR FALSE

- » A high advertised yield proves that a protocol can provide greater return without increasing uncertainty, dependency, or possible loss.

SHORT EXPLANATION

- » In five or six sentences, explain how a DeFi protocol can use smart contracts to automate a financial function while still depending on people, market liquidity, oracles, governance, and outside organizations.



SUMMARY AND PRACTICAL TAKEAWAYS

- » DeFi is a broad category of blockchain-based services, not one product or organization.
- » DeFi can perform exchange, lending, borrowing, and liquidity functions through smart contracts.
- » A decentralized label does not describe who controls every layer.
- » A DEX can reduce reliance on centralized custody while introducing code, interface, liquidity, and personal-security risks.
- » An automated market maker calculates exchanges from a formula and pool balances.
- » A pool price is not proof of fair economic value.
- » Larger trades can have greater price impact in a shallow pool.
- » Liquidity providers may receive fees or incentives while remaining exposed to token-price changes and contract risk.
- » The independent PP/WBNB pair provides a non-promotional example of two tokens held in a BNB Smart Chain liquidity pool.
- » The PP token, DEX pair, interface, block explorer, treasury, community website, and Prison Professors organization are separate components.
- » DeFi lending often relies on pooled assets and overcollateralized borrowing.
- » Collateral can fall in value and become eligible for liquidation.
- » Liquidation protects a protocol's collateral position but can cause a borrower an involuntary loss.
- » Oracles provide price information that can directly affect borrowing and liquidation.
- » Yield may come from borrower interest, trading fees, incentive tokens, a treasury, or another strategy.
- » A yield percentage is incomplete without its source, conditions, payment asset, fees, and possible loss.
- » Available liquidity can limit an exchange or withdrawal.
- » Stablecoins, wrapped assets, bridges, and connected protocols add dependencies.
- » Governance and administrative powers can support repairs while concentrating control.
- » Audits and public records offer bounded evidence rather than guarantees.



- » Greater possible return should lead to deeper questions about the system that creates it.
- » No course activity requires financial participation.

The practical takeaway is to map the system before evaluating the promise. Identify the function, assets, source of return, controls, loss pathways, exit conditions, evidence, and unknowns.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a clear explanation:

- » Define decentralized finance in your own words.
- » Explain how a decentralized exchange and liquidity pool can support a token exchange.
- » Use the independent PP/WBNB pair or the fictional RiverBridge scenario to identify the assets, smart contracts, pricing or lending rules, and human controls.
- » Explain the role of collateral and why a decline in its value can produce liquidation.
- » Identify at least three possible sources of yield and explain why each source carries conditions.
- » Describe one liquidity risk and one oracle risk.
- » Explain why the word decentralized does not prove that control is evenly distributed.
- » Answer the Profile focus: Why should a promise of greater return lead to more questions rather than greater confidence?
- » Connect the lesson to your own self-directed learning. Describe how you can examine an opportunity carefully, document your reasoning, and seek evidence before reaching a conclusion.

Your response should demonstrate technical understanding, critical thinking, and personal responsibility. Do not visit a website, connect a wallet, create an account, acquire an asset, provide liquidity, borrow, lend, or perform a transaction. Do not include any real password, private key, seed phrase, authentication code, wallet address, balance, transaction identifier, or financial-account information.



SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 17: Decentralized Finance, and the date you completed the entry.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 17 — [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 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 identifiers, transaction details, or other sensitive information in a Profile response.

UNDERSTANDING WEB3

LESSON 18: DECENTRALIZED ORGANIZATIONS AND GOVERNANCE

A Prison Professors Self-Directed Course

Estimated time: 75–110 minutes**Educational and Safety Boundary:**

This lesson provides general education about decentralized organizations, governance, voting systems, and related risks. It does not provide individualized financial, investment, legal, tax, organizational, or voting advice. No activity requires internet access, an account, a wallet, a digital asset, or a transaction. Opening Guidance

While serving 26 years in federal prison, I learned that a written plan has value only when people understand it, carry it out, review the results, and accept responsibility for what follows. A schedule could organize my study time, but it could not make me study. A goal could guide my choices, but it could not make the choices for me.

Blockchain communities face a similar challenge. Smart contracts can record proposals, count voting power, restrict treasury access, and execute approved instructions. Those tools can create a visible process. They cannot guarantee informed participation, fair influence, wise decisions, honest leadership, or responsible use of resources.

People often use the phrase decentralized autonomous organization, or DAO, to describe a community that coordinates through blockchain tools. The name can create two misunderstandings. Decentralized does not prove that influence is broadly distributed. Autonomous does not prove that the organization operates without people.

People still write proposals, persuade voters, delegate authority, maintain code, interpret rules, control interfaces, respond to emergencies, and complete work outside the blockchain. If a community approves funding for an educational program, code may transfer the approved tokens. People must still create the lessons, serve participants, document outcomes, and account for the resources.

The independent PP token community gives us a useful recurring example. Neither Prison Professors nor I created, organized, managed, or controlled that token project. The community formed independently and connected its work with our mission. Its token, public communications, and visible on-chain activity show that people can organize around a shared purpose. Those features do not by themselves prove that the community is a DAO or explain how its decisions are made.

PURPOSE AND ESSENTIAL QUESTION

Lesson 18 explains how blockchain communities may organize proposals, voting, resources, and decision-making. It introduces governance tokens, voting power, delegation, treasuries, quorum, execution, and the risks created by low participation or concentrated influence.

Essential Question:

- » What makes a decision-making process responsible, transparent, and fair?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Define decentralized autonomous organization and governance token.
- » Describe a basic proposal and voting process.
- » Identify participation, concentration, delegation, security, legal, and accountability challenges.
- » Evaluate whether formal voting power produces meaningful decentralization.

KEY TERMS

DECENTRALIZED AUTONOMOUS ORGANIZATION

Definition: A community or organization that uses blockchain-based rules, smart contracts, and collective decision procedures to coordinate selected activities, resources, or protocol changes. The abbreviation is DAO.

Sample sentence: The decentralized autonomous organization required a public proposal and vote before its treasury could fund the project.

GOVERNANCE

Definition: The rules, roles, and processes used to make decisions, assign authority, resolve disagreements, and hold participants accountable.

Sample sentence: The community's governance process explained who could propose a change, who could vote, and how an approved action would be carried out.

GOVERNANCE TOKEN

Definition: A token designed to represent or help calculate voting power in a blockchain-based governance system.

Sample sentence: The governance token gave holders voting units, but the distribution of those units affected how widely influence was shared.

PROPOSAL

Definition: A documented recommendation asking a community or governance system to approve a defined decision or action.

Sample sentence: The proposal identified the requested treasury amount, intended recipient, timeline, risks, and method for reporting results.

VOTING POWER

Definition: The amount of influence an account, person, or delegate can apply to a vote under the system's rules.

Sample sentence: One account held enough voting power to defeat a proposal supported by many smaller participants.

DELEGATION

Definition: The assignment of voting power to another person or account that may vote as a representative, generally without transferring ownership of the underlying token.

Sample sentence: The holder used delegation so that a representative with more time could review proposals and cast informed votes.

TREASURY

Definition: Resources controlled for a community or organization and used according to its approved rules.

Sample sentence: The treasury released funds only after the proposal passed, the waiting period ended, and the authorized transaction was executed.

MAIN LESSON

A DAO IS AN ORGANIZATION SUPPORTED BY TOOLS

A DAO may use smart contracts to manage selected rules and resources. The tools can create public records and automate narrow actions. The organization still depends on people.



PEOPLE MAY:

- » Define the mission.
- » Decide who can participate.
- » Write and discuss proposals.
- » Choose a voting method.
- » Delegate voting power.
- » Review code and financial effects.
- » Vote or abstain.
- » Maintain interfaces and communication channels.
- » Perform approved work.
- » Resolve conflicts and respond to failures.

The balance between code and people differs across organizations. One DAO may place treasury control behind an on-chain vote and timelock. Another may use an off-chain poll to advise a multisignature group. A third may call itself a DAO while a small development team retains broad administrative power.

The label does not establish the design. A responsible learner asks which decisions occur on-chain, which occur off-chain, who controls each step, and what evidence shows that the published process is followed.

“AUTONOMOUS” HAS LIMITS

In a governance setting, autonomous commonly refers to code carrying out defined rules without asking a conventional manager to approve each transaction. For example, a governor contract may accept a proposal, record votes, determine whether quorum was reached, place a successful action into a time delay, and later allow execution.

The code does not create the proposal’s purpose. It does not examine every social consequence. It does not confirm that voters read the supporting information. It does not supervise the person who receives a grant. It cannot create a fair exception unless the rules include one.

A DAO can automate an authorization process while retaining human judgment throughout the larger system. That distinction keeps learners from treating code as leadership.

GOVERNANCE TOKENS AND VOTING POWER

A governance token may represent voting units. In a simple token-weighted design, one token provides one unit of voting power. A person or organization holding more tokens can exert more influence.

Token-weighted voting can be easy to calculate and verify on a blockchain. It can also create concentration. Founders, early participants, investors, a treasury, or a small number of large holders may control enough voting power to submit proposals, reach quorum, block changes, or determine outcomes.

Token ownership and voting power are not always identical. A holder may need to delegate voting power to the holder's own address before voting. A holder may instead delegate to a representative. A system may measure voting power at a recorded snapshot so that later token transfers do not change the weight used for an active proposal.

A governance token may have market value, voting use, or both. Voting rights do not guarantee ownership of a legal entity, a share of revenue, a right to treasury assets, or protection from loss. The actual rights depend on the system's documents, code, facts, and applicable law.

OTHER VOTING DESIGNS

Not every governance system uses one-token-one-vote.

One-person-one-vote can give each verified member equal formal influence. It creates an identity challenge in an open digital system: how does the community prevent one person from creating many identities?

Reputation-based voting may give greater influence to contributors with a record of service. The community must decide who measures contribution, how records can be corrected, and whether past influence becomes too difficult to challenge.

Role-based voting may give selected decisions to technical reviewers, elected councils, safety committees, or grant teams. This can improve expertise and speed while concentrating authority.

Some systems combine methods. Token holders may elect delegates. Delegates may review proposals. A security council may have limited emergency powers. A timelock may delay execution. The community may require public reporting after treasury funds are used.

No voting design produces fairness automatically. Each design chooses which values to emphasize, such as equal membership, financial exposure, contribution, expertise, speed, resistance to manipulation, or broad participation.

THE PROPOSAL LIFECYCLE

A formal governance process commonly moves through several stages:

1. Idea and discussion. A participant describes a problem, seeks feedback, and revises the concept.
2. Written proposal. The proposer states the requested action, reasons, costs, risks, conflicts, timeline, and expected result.
3. Eligibility review. The system checks whether the proposer satisfies any threshold and whether the proposal follows required format and scope.
4. Voting delay or review period. Participants receive time to study the final proposal and arrange delegation.
5. Voting period. Eligible voters cast support, opposition, or abstention according to the system's rules.
6. Count and quorum. The system evaluates voting power, participation, and the rule for success.
7. Queue and timelock. A successful proposal may wait before execution so participants can review the approved action or respond to a discovered problem.
8. Execution. An authorized account or smart contract performs the approved on-chain actions.
9. Reporting and accountability. People document how resources were used, whether the intended work occurred, and what the community learned.

Different systems use different stages. Some votes only express community preference and require people to act afterward. Other proposals contain executable instructions that can change protocol settings or transfer treasury assets after approval.

A proposal should distinguish the human-readable explanation from the executable action. A description can sound reasonable while attached code does something else. Technical reviewers may need to verify that the requested calls match the stated purpose.

PROPOSAL THRESHOLDS AND QUORUM

A proposal threshold is the minimum voting power or other qualification required to submit a formal proposal. It can reduce spam and prevent the system from reviewing endless low-quality requests. A threshold set too high can prevent smaller participants from placing useful ideas before the community.



Quorum is the minimum participation required before a vote can produce a valid outcome. It is intended to prevent a small number of active voters from deciding for an inactive community.

Quorum creates tradeoffs. A low requirement may allow a small group to control decisions. A high requirement may cause reasonable proposals to fail because many eligible voters do not participate. A large holder may have enough voting power to reach quorum alone or prevent others from reaching it.

A vote can satisfy every formal rule while still showing weak decentralization. If three accounts hold most voting power, the outcome may reflect those accounts even when hundreds of smaller holders participate.

DELEGATION CAN IMPROVE PARTICIPATION AND CONCENTRATE INFLUENCE

Governance can require time and knowledge. Participants must read proposals, understand technical effects, identify conflicts, and follow changes. Many holders will not complete that work for every vote.

Delegation allows a holder to assign voting power to a representative without transferring the underlying asset. A capable delegate can study proposals, explain reasoning, and vote consistently. Delegation can help people who lack time, technical knowledge, or access.

DELEGATION ALSO CREATES RISKS:

- » Many holders may choose the same well-known delegate.
- » A delegate may receive enough power to dominate proposals or outcomes.
- » A delegate may have an undisclosed conflict.
- » A representative may vote without explaining the decision.
- » Holders may stop reviewing the delegate's record.
- » Incentives may encourage votes that benefit the delegate rather than the community.
- » A compromised delegate account may place substantial voting power at risk.

Responsible delegation requires transparency. A delegate should disclose interests, publish reasoning, participate consistently, protect credentials, and accept that delegators can withdraw their authority.



TREASURIES CONNECT VOTING WITH RESOURCES

A DAO treasury may hold tokens or other digital assets intended for grants, development, operations, reserves, or public purposes. Smart contracts can restrict access so that resources move only after approved conditions are satisfied.

Public treasury records can help people observe incoming and outgoing transactions. They do not explain every decision or prove that off-chain work occurred. A transfer shows that assets moved to an address. It does not by itself identify the person who ultimately controlled the resources, establish the quality of the work, or confirm that the community received the promised result.

Responsible treasury governance may require:

- » A clear budget and purpose.
- » Conflict-of-interest disclosure.
- » Named or verifiable responsibility for deliverables.
- » Milestones or staged payments.
- » Independent review for large requests.
- » A waiting period before execution.
- » Records connecting on-chain transfers with off-chain invoices, reports, or outcomes.
- » A process for unused resources, failed work, and disputes.

Treasury transparency should connect authorization, transaction records, and performance reporting.

TIMELOCKS AND EMERGENCY POWERS

A timelock creates a delay between approval and execution. The delay can give participants time to inspect the final action, identify a hidden error, withdraw from a protocol, or organize a response.

A delay cannot correct a harmful proposal by itself. The system needs a lawful and authorized way to cancel, pause, or replace the action when a serious defect appears.

Some systems give a guardian, council, multisignature group, or administrator limited emergency power. That authority may help stop an exploit quickly. It can also concentrate control.

EVALUATE:

- » Which actions can be paused?
- » Who holds the emergency authority?



- » Can the authority move treasury assets or only stop functions?
- » How many independent approvals are required?
- » How long does the power last?
- » Must the community ratify or review the emergency action?
- » Are actions and reasons published?

Safety and decentralization can pull in different directions. A system should state the tradeoff clearly.

PARTICIPATION IS MORE THAN CASTING A VOTE

Meaningful governance requires more than counting ballots. Participants need understandable proposals, enough review time, reliable information, accessible discussion, and a practical opportunity to influence the result.

A voting interface may be open while participation remains narrow because transaction fees, language, technical complexity, internet access, time zones, disability barriers, or lack of information exclude people. Token holders may remain inactive because they believe large holders have already determined the outcome.

Participation quality also counts. A high turnout can still produce weak governance when voters follow a promoter, accept an undisclosed payment, misunderstand the executable action, or vote without reviewing the proposal.

USEFUL GOVERNANCE RECORDS MAY SHOW:

- » The proposal and all revisions.
- » Supporting and opposing arguments.
- » The identity or declared role of the proposer.
- » Conflicts and financial interests.
- » Voting-power distribution.
- » Delegate statements and voting history.
- » Quorum and final counts.
- » The executable action.
- » The time and result of execution.
- » Follow-up reports.

Transparency improves the opportunity for review. It does not guarantee that participants use the information well.



CONCENTRATION CAN HIDE BEHIND FORMAL VOTING

Imagine a community with 1,000 token holders. If five accounts control 70 percent of active voting power, the community may have broad membership and narrow authority.

CONCENTRATION CAN ARISE THROUGH:

- » Unequal token distribution.
- » Low participation among smaller holders.
- » Delegation to a few representatives.
- » Treasury-controlled voting units.
- » Founder or investor allocations.
- » Vote-buying or temporary incentives.
- » Cross-holdings among related organizations.
- » Technical proposal thresholds that only large delegates can satisfy.

The number of wallets does not equal the number of independent people. One person can control several wallets, while one wallet can represent many people or an organization. Blockchain records show addresses and voting units; additional evidence may be needed to understand real control.

Meaningful decentralization is a question of distribution, participation, independence, checks, and accountability—not only the existence of a voting contract.

GOVERNANCE ATTACKS AND SECURITY RISKS

A governance system may control valuable contracts and treasuries. Attackers can target the decision process rather than only the application code.

POSSIBLE ATTACKS AND FAILURES INCLUDE:

- » Acquiring or borrowing enough voting power to influence a proposal.
- » Hiding a harmful action inside a complicated proposal.
- » Compromising a delegate, administrator, or multisignature signer.
- » Manipulating an off-chain discussion or voting interface.
- » Creating many false identities in a one-person voting system.
- » Bribing voters or delegates.
- » Exploiting a defect in the governor, token, timelock, or treasury contract.
- » Rushing a proposal through before participants can review it.
- » Preventing quorum or execution through coordinated inaction.

Snapshots, proposal thresholds, review periods, timelocks, multiple signers, audits, and public debate can reduce selected risks. Each control also adds complexity or creates a new authority.

ACCOUNTABILITY DOES NOT END AT EXECUTION

An approved vote authorizes an action under the system's rules. It does not prove that the action is wise, ethical, lawful, or successful.

ACCOUNTABILITY ASKS:

- » Who wrote the proposal?
- » Who benefited?
- » Who reviewed the risks?
- » Who voted and with how much influence?
- » Who performed the approved work?
- » What evidence shows the intended result?
- » Who can investigate a failure?
- » What remedy or correction process exists?

A community can publish every vote and still fail to explain a conflict or report an outcome. Public records are strongest when they connect with clear human responsibility.

LEGAL STATUS AND RESPONSIBILITY

The word DAO does not automatically create a recognized legal entity, limit liability, define ownership, or remove regulatory duties. Legal treatment depends on the organization's activity, participants, jurisdiction, economic structure, and other facts.

In a 2017 United States report about a specific project called The DAO, the Securities and Exchange Commission concluded that the tokens offered and sold in that arrangement were securities under the facts it examined. That finding should not be converted into a claim that every governance token or DAO is the same. It demonstrates that a technology label does not replace analysis of the actual arrangement.

DAO participants may face questions involving contracts, securities, tax, employment, intellectual property, consumer protection, privacy, fiduciary duties, sanctions, or other laws. The relevant questions vary. A person or organization should seek qualified advice for a real arrangement.

APPLIED CASE: COMMUNITY SUPPORT DOES NOT AUTOMATICALLY CREATE A DAO

The independent PP token community formed without direction or control from Prison Professors or CZ. Its members created a token, communicated through public channels, and connected part of the token's programmed activity with a public mission treasury. That independent effort shows how people who did not previously know our team can discover documented work and choose to support it.

The story can inspire learners to build a record of disciplined preparation. It also gives us an opportunity to apply governance analysis accurately.

A token does not automatically create a governance system. A public treasury address does not automatically show who can authorize future use. A Telegram group does not automatically define membership or voting rights. A smart contract does not automatically establish a legal organization.

Before describing any community as a DAO, I would look for evidence addressing these questions:

- » Who may submit a proposal?
- » Which decisions are subject to voting?
- » Who may vote?
- » How is voting power calculated?
- » Can voting power be delegated?
- » What quorum and approval rules apply?
- » Who can change the rules or contracts?
- » Who controls emergency powers?
- » How is the treasury authorized and protected?
- » How are off-chain mission decisions reviewed and reported?
- » How are conflicts disclosed?
- » What legal or organizational structure, if any, supports the activity?

The current course case does not need answers to all those questions. Its purpose is to teach us not to infer a governance structure from a token or public balance alone.

If a community later adopted formal proposal, voting, delegation, and reporting procedures, learners could compare the published rules with actual records. Until evidence supports that description, the accurate language is independent token community rather than DAO.

APPLIED SCENARIO: THE SECOND CHANCE LEARNING TREASURY

The following scenario is fictional and requires no device, account, token, or transaction.

A group called the Second Chance Learning Network wants to fund educational materials. It creates a paper model of a DAO before considering any technology. The group has ten members and a treasury of 100 learning credits. The credits have no cash value and exist only for this exercise.

A member proposes spending 30 treasury credits to produce a new workbook. The proposal includes the purpose and amount but does not identify the writer, delivery date, quality standard, conflict disclosures, payment stages, or reporting requirement.

THE GOVERNANCE RULES SAY:

- » At least 50 voting units must participate for quorum.
- » More voting units must support than oppose the proposal.
- » Abstentions count toward quorum but not toward support or opposition.
- » A successful proposal waits seven paper-days before execution.
- » One guardian can pause execution for a suspected security problem.
- » No rule requires the guardian to publish a reason or obtain later community review.

Voting power is distributed as follows:

- » Member A: 40 units.
- » Member B: 20 units.
- » Member C: 10 units.
- » Member D: 10 units.
- » Member E: 5 units.
- » Member F: 5 units.
- » Member G: 3 units.
- » Member H: 3 units.
- » Member I: 2 units.
- » Member J: 2 units.

Members A and B oppose the proposal. Members C through J support it.

Under one-person-one-vote, eight members support and two oppose. Under the token-weighted rules, 40 units support and 60 oppose. The same people reach opposite results under two different definitions of voting power.

The scenario exposes several governance questions. The proposal is incomplete. Two people control most voting power. The guardian has broad discretion without a reporting rule. The community can see the vote, but it still needs evidence that funded work is completed.

A better proposal could name the responsible party, disclose relationships, define milestones, split payment into stages, specify review criteria, require a completion report, and explain what happens if the work is late or incomplete.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Public proposals and voting records can support transparent review.
- » Smart contracts can enforce thresholds, voting periods, quorum, delays, and approved on-chain actions.
- » A treasury can require collective authorization rather than one person's signature.
- » Delegation can help participants choose informed representatives.
- » Timelocks can provide review time before approved actions execute.
- » Communities can coordinate people across institutions and locations.
- » Written governance rules can clarify authority and accountability even when a blockchain is not used.

LIMITATIONS AND RISKS

- » Voting power may be concentrated among founders, investors, treasuries, or large delegates.
- » Low participation can allow a small group to control outcomes or prevent quorum.
- » One person may control several addresses, while one address may represent many people.
- » A proposal description may not match its executable instructions.
- » Delegates can have conflicts, poor participation, weak security, or excessive influence.
- » Governance contracts, tokens, treasuries, timelocks, and interfaces can contain defects.
- » Emergency powers can support safety while concentrating authority.
- » Public votes can create pressure, retaliation, bribery, or privacy concerns.

- » Treasury transactions do not prove that off-chain work was completed.
- » A successful vote does not establish ethical, legal, or practical success.
- » The legal status and duties of a DAO or its participants can be uncertain.

COMMON MISCONCEPTIONS

- » “A token community is automatically a DAO.” A community needs defined governance rules, authority, and evidence of how decisions are made.
- » “Autonomous means no people are involved.” People design, propose, review, vote, maintain, execute, and complete off-chain work.
- » “One token equals one person.” One person can control many addresses or tokens, and one address can represent many people.
- » “More voters always means more decentralization.” A few large accounts can outweigh many smaller participants.
- » “Delegation spreads power.” Delegation can improve representation or concentrate power among a small number of delegates.
- » “A public treasury is fully accountable.” The blockchain shows selected transfers, while human reporting must explain purpose, recipients, performance, and results.
- » “A passed proposal is automatically wise.” Formal approval does not prove accurate information, good judgment, or a beneficial outcome.
- » “A timelock prevents harmful actions.” A delay creates review time; people still need authority and a process to respond.
- » “Code eliminates leadership.” Governance still requires judgment, communication, maintenance, conflict resolution, and responsibility.
- » “A DAO label removes legal duties.” Legal treatment depends on facts, activities, participants, and jurisdiction.

OFFLINE EXERCISE: COMPARE GOVERNANCE POWER

Estimated time: 30–35 minutes

Materials: Separate paper and a pencil.

Use the fictional Second Chance Learning Treasury. Do not use a website, wallet, account, token, or real asset.

1. Copy the ten-member voting-power distribution and confirm that it totals 100 units.
2. Record each member’s position on the workbook proposal.



3. Calculate the result under one-person-one-vote.
4. Calculate the result under the stated token-weighted rules.
5. Explain why the same participants produce different outcomes.
6. Suppose only Members C through J vote. Determine whether their 40 voting units reach the 50-unit quorum.
7. Suppose only Members A and B vote. Determine whether their 60 voting units reach quorum and what result follows.
8. Explain how two members can produce a valid outcome while eight members cannot produce one under the stated distribution.
9. Now assign ten equal voting units to each member. Recalculate the result and explain how the distribution changed the outcome.
10. Assume Members E through J delegate their combined 20 voting units to Member C. Explain one possible benefit and two risks of that delegation.
11. Identify five missing details in the workbook proposal that voters should request before authorizing treasury resources.
12. Rewrite the guardian rule so that emergency action has a narrow scope, a published reason, a time limit, and later community review.

Finish with one paragraph of six to eight sentences:

What makes a decision-making process responsible, transparent, and fair? Address participation, distribution of influence, understandable information, conflicts, security, execution, and follow-up reporting.

The exercise does not ask you to choose a perfect voting system. It asks you to identify how different rules distribute authority and shape outcomes.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which description best fits a decentralized autonomous organization?
 - a. A group in which software replaces every human decision
 - b. A community that uses blockchain-based rules and collective procedures to coordinate selected decisions or resources
 - c. Any online group that discusses a token
 - d. A legal entity with identical status in every jurisdiction
2. What is delegation?
 - a. Transferring ownership of all tokens to a centralized exchange



- b. Assigning voting power to a representative under the governance rules
- c. Guaranteeing that a delegate will vote correctly
- d. Eliminating the need for voters to review a delegate's conduct
- 3. Why can token-weighted voting remain concentrated?
 - a. Every token always represents a different person
 - b. Larger holders or delegates may control a high percentage of active voting power
 - c. Quorum always gives each participant equal influence
 - d. Public records prevent related accounts from coordinating

TRUE OR FALSE

- » A successful on-chain vote proves that an approved proposal is fair, lawful, secure, and effective.

SHORT EXPLANATION

- » In five or six sentences, explain why a token, a public treasury, and a community communication channel do not by themselves prove that a community has responsible DAO governance.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A DAO uses blockchain tools and collective procedures to coordinate selected decisions or resources.
- » People remain responsible for mission, proposals, participation, implementation, and accountability.
- » A governance token may help calculate voting power without guaranteeing equal influence or legal rights.
- » One-token-one-vote can make calculation simple while concentrating authority.
- » Other designs may emphasize equal membership, reputation, roles, or combinations of methods.
- » A proposal lifecycle can include discussion, written terms, review, voting, quorum, a timelock, execution, and reporting.
- » A proposal threshold can reduce spam while excluding smaller participants.
- » Quorum can protect against low participation while giving large holders special influence.
- » Delegation can improve informed participation or concentrate authority among a few representatives.



- » A public treasury record shows selected transfers, not the quality or completion of off-chain work.
- » Timelocks create review time but do not correct harmful actions by themselves.
- » Emergency powers can support safety and create centralization risk.
- » Meaningful participation requires understandable information and a practical opportunity to influence outcomes.
- » Wallet counts do not establish how many independent people control voting power.
- » Governance attacks can target voters, delegates, proposals, interfaces, contracts, and treasuries.
- » A completed vote authorizes an action under the rules; it does not prove success or responsibility.
- » DAO legal treatment depends on the actual arrangement and applicable law.
- » The independent PP token community should not be described as a DAO without evidence of formal governance.
- » Different voting distributions can produce opposite outcomes from the same member preferences.
- » Responsible governance connects transparent authorization with execution and follow-up reporting.
- » No course activity requires digital participation.

The practical takeaway is to examine authority rather than labels. Ask who can propose, who can vote, how influence is distributed, how decisions execute, what safeguards apply, and who reports the result.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a clear explanation:

- » Define a DAO and governance token in your own words.
- » Describe the stages of a responsible proposal and voting process.
- » Explain the difference between membership count and voting-power distribution.
- » Use the Second Chance Learning Treasury scenario to compare one-person-one-vote with token-weighted voting.
- » Explain one benefit and two risks of delegation.



- » Describe how quorum, a timelock, and limited emergency authority can support governance.
- » Explain why public treasury transfers require off-chain performance reporting.
- » Use the independent PP token community case to explain why a token and public community do not automatically establish a DAO.
- » Answer the Profile focus: What makes a decision-making process responsible, transparent, and fair?
- » Connect the lesson to your own self-directed learning. Explain how you can document decisions, seek feedback, disclose conflicts, and accept responsibility for results.

Your response should demonstrate technical understanding, critical thinking, and personal responsibility. Do not visit a website, connect a wallet, create an account, acquire an asset, delegate voting power, join a DAO, or perform a transaction. Do not include any real password, private key, seed phrase, authentication code, wallet address, balance, transaction identifier, or financial-account information.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 18: Decentralized Organizations and Governance, and the date you completed the entry.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 18 — [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 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 identifiers, transaction details, or other sensitive information in a Profile response.



UNDERSTANDING WEB3

SECTION 5 REVIEW: SMART CONTRACTS, DEFI, AND GOVERNANCE

A Prison Professors Self-Directed Course

Estimated time: 75–105 minutes

Educational Boundary:

This review provides general education about technology, financial systems, governance, and risk. It does not provide individualized financial, investment, legal, tax, programming, organizational, or voting advice.

REVIEW PURPOSE

You have completed Lessons 16 through 18 of Understanding Web3. This review gives you a place to connect smart-contract logic, decentralized-finance systems, and blockchain governance. Each topic introduces its own risks. When the topics operate together, one weakness may affect several parts of the system.

I encourage you to use the review as a systems-analysis exercise. Begin with the rules the code can execute. Then trace the assets, data, people, permissions, and decision procedures connected with those rules. A disciplined review asks what a system can do, what it depends on, who can change it, who may benefit, and who may absorb a loss.

THE REVIEW COVERS:

- » How smart contracts use inputs, rules, stored state, and outputs, and how a decentralized application connects several technical and human layers.
- » How oracles, audits, administrative controls, interfaces, and vulnerabilities affect automated execution.
- » How decentralized exchanges, liquidity pools, lending, collateral, liquidation, and yield create connected benefits and risks.
- » How governance tokens, proposals, voting power, delegation, treasuries, timelocks, participation, and accountability influence collective decisions.
- » How to evaluate a system that combines code, financial exposure, and governance authority.

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 smart contract?
 - a. A person who negotiates blockchain agreements for a community
 - b. Code deployed on a blockchain that stores data and performs defined functions when called
 - c. A guarantee that every programmed transaction is lawful and fair
 - d. A private database that only its original programmer can inspect
2. Which description offers the most complete view of a decentralized application?
 - a. Only the website or screen that a user sees
 - b. Only the smart contract recorded on a blockchain
 - c. A combination that may include an interface, smart contracts, a network, wallets, outside data, and human controls
 - d. Any financial service that uses the word decentralized
3. A lending contract relies on an oracle for the price of collateral. What risk follows from that design?



- a. The blockchain can independently confirm every outside price without any data source.
 - b. Incorrect, delayed, or manipulated oracle data may trigger an incorrect financial result.
 - c. An oracle prevents every coding defect in the lending contract.
 - d. The use of an oracle guarantees that collateral cannot lose value.
4. What role does a liquidity pool commonly serve on a decentralized exchange?
- a. It supplies tokens that a smart contract may use to support exchanges.
 - b. It guarantees a fixed market price for every token.
 - c. It gives a central help desk the power to reverse every exchange.
 - d. It proves that every token in the pool has a lawful purpose.
5. A borrower's collateral falls below a protocol's required threshold. Which result may follow?
- a. The protocol may make the position eligible for liquidation under its rules.
 - b. The borrower automatically receives more collateral at no cost.
 - c. The network must cancel the original borrowing transaction.
 - d. The advertised yield becomes guaranteed.
6. Before accepting a claim that a protocol offers high yield, which question is most useful?
- a. Does the website use professional graphics?
 - b. How many times does the community use the word opportunity?
 - c. What produces the return, what conditions support it, and what paths could lead to loss?
 - d. Can the protocol promise that market prices will rise?
7. Which statement best describes delegation in blockchain governance?
- a. It permanently transfers ownership of every token to the delegate.
 - b. It assigns voting power to a representative under the system's rules and may improve participation while concentrating influence.
 - c. It removes the need to examine a representative's incentives or conflicts.
 - d. It guarantees that every participant has equal influence.

TRUE OR FALSE

- » A prior code audit guarantees that a decentralized application, its oracle, its interface, and every later upgrade are safe.



- » A token-weighted vote may follow published rules while a small number of addresses still hold enough voting power to control the outcome.

SHORT EXPLANATION

- » A proposal describes a protocol as “audited,” “community controlled,” and able to produce an 18 percent annual yield. In five to seven sentences, explain what those phrases may indicate, what they do not establish, and which evidence you would examine before reaching a conclusion.

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. Smart contract
- b. Decentralized application
- c. Oracle
- d. Audit
- e. Vulnerability
- f. Decentralized finance
- g. Decentralized exchange
- h. Liquidity pool
- i. Collateral
- j. Liquidation
- k. Yield
- l. Decentralized autonomous organization
- m. Governance token
- n. Delegation
- o. Treasury

DEFINITIONS

- 1. Resources controlled for a community or organization and used according to its approved rules.
- 2. A service or system that supplies a blockchain application with information from outside the blockchain.

3. Tokens placed in a smart contract so that a protocol can support exchanges, loans, or other functions.
4. A return associated with providing, lending, staking, or otherwise committing an asset; it may come from several sources and is not guaranteed profit.
5. A community or organization that uses blockchain-based rules, smart contracts, and collective decision procedures to coordinate selected activities or resources.
6. A program deployed at an address on a blockchain that stores data and performs defined functions when called.
7. A structured technical review intended to identify defects and security weaknesses within a stated scope.
8. An asset pledged to support an obligation and exposed to being taken or sold if required conditions are not maintained.
9. A blockchain-based protocol that allows token exchanges through smart contracts rather than relying only on a conventional exchange's internal ledger.
10. The assignment of voting power to another person or account that may vote as a representative, generally without transferring ownership of the underlying token.
11. A weakness in code, design, configuration, data, or operations that could cause failure or allow misuse.
12. A broad term for blockchain-based services that use smart contracts to perform financial-like functions.
13. A token designed to represent or help calculate voting power in a blockchain-based governance system.
14. An application that uses one or more smart contracts on a decentralized network and usually includes an interface and supporting components.
15. A process that sells or transfers collateral after a borrowing position crosses a defined risk threshold.

PART 3: APPLIED SCENARIO — THE OPENPATH LEARNING POOL

This scenario is fictional. OpenPath, StudyDollar, PathToken, and PathGov do not represent verified products or assets. The figures exist only for analysis. No learner should acquire an asset, create an account, connect a wallet, or conduct a transaction to complete this exercise.

A community launches the OpenPath Learning Pool, a decentralized application that uses several smart contracts. Supporters may supply a fictional token called



StudyDollar. The protocol lends some of those tokens to borrowers and describes a variable yield for suppliers. The stated sources of the yield are interest paid by borrowers and newly distributed PathGov reward tokens.

Borrowers pledge a volatile fictional asset called PathToken as collateral. A price oracle reports the value of that collateral. If the reported value falls below the required threshold, a smart contract may liquidate the position. During periods of heavy withdrawals, suppliers can receive StudyDollar only when enough tokens remain available in the pool.

PathGov tokens also provide voting power. Token holders may submit proposals, delegate votes, change financial settings, approve upgrades, and direct the community treasury. The two largest addresses hold 64 percent of the recorded voting power. Many smaller holders do not vote. One widely followed delegate is paid as a consultant by companies that seek protocol work, but the governance page does not require the delegate to disclose those relationships.

A new proposal combines four changes: replace the price oracle, lower the collateral requirement, transfer 250,000 StudyDollar from the treasury to a company owned by the proposal's author, and reduce the waiting period before execution from 48 hours to two hours. The proposal summary says the package will create "safer data and higher yield." It does not include financial simulations, an independent review of the new oracle, a conflict disclosure, or separate votes on the four changes.

The application's website says that OpenPath is "audited and community controlled." The audit is one year old, covers an earlier version of the lending contract, and excludes the website interface, oracle, current upgrade code, and administrative keys. A three-person emergency committee can pause the protocol, and two committee members can approve an upgrade. The public description does not identify how the committee members were selected or how their decisions are reviewed.

The proposal reaches the minimum quorum. Most participating addresses support it, but the two largest addresses supply nearly all of the favorable voting power. If the proposal executes after two hours, its code will change the oracle, collateral threshold, treasury balance, and future execution delay in one action.

SCENARIO QUESTIONS

1. Identify the principal parts of the decentralized application. Separate the user interface, smart contracts, blockchain network, wallet interactions, oracle, administrative controls, and human governance. Explain how a failure in one part could affect another.

2. Use the input–rule–state–output model to describe the liquidation process. Identify the oracle input, the collateral rule, the stored borrowing position, and the possible output. Explain how incorrect data or faulty code could change the result.
3. Trace the proposed yield to its stated sources. Then identify at least five ways a supplier could receive less than expected or lose access to deposited tokens. Include liquidity, borrower, collateral, oracle, token-incentive, smart-contract, and governance risks where relevant.
4. Evaluate the governance process. Discuss voting concentration, low participation, delegation, the consultant relationship, quorum, the bundled proposal, and the difference between the number of participating addresses and the amount of voting power behind the outcome.
5. Evaluate the claims “audited,” “community controlled,” “safer data,” and “higher yield.” For each claim, identify the evidence supplied, the gaps that remain, and the additional information a careful reviewer would request.
6. Propose a more responsible review and approval process before any change executes. Address separate proposals, conflict disclosure, current technical review, oracle testing and fallback procedures, collateral and liquidity analysis, treasury authorization, voting concentration, a useful waiting period, emergency powers, and public reporting after execution.

COMPLETION CHECK

Before moving to Section 6, ask yourself whether you can:

- » Explain what smart-contract code can automate and which decisions still depend on people, data, interfaces, permissions, and governance.
- » Describe a decentralized application as a set of connected layers rather than as only a website or contract.
- » Trace how a decentralized exchange, liquidity pool, lending system, collateral rule, liquidation process, and proposed yield may work.
- » Identify smart-contract, oracle, liquidity, volatility, collateral, governance, administrative, fraud, and legal risks.
- » Evaluate governance by examining proposals, voting power, delegation, participation, treasuries, execution, conflicts, and accountability.
- » Analyze how one decision can create technical, financial, and governance consequences across a connected system.



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 5 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 5 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.

UNDERSTANDING WEB3**LESSON 19: REAL-WORLD APPLICATIONS, LIMITATIONS, AND CAREER SKILLS**

A Prison Professors Self-Directed Course

Estimated time: 80–115 minutes

Educational and Safety Boundary:

This lesson provides general education about blockchain applications, transferable abilities, career preparation, and related risks. It does not provide individualized financial, investment, legal, tax, employment, credentialing, or career advice. No activity requires internet access, an account, a wallet, a digital asset, a purchase, or a transaction. Opening Guidance

During 26 years in federal prison, I learned that preparation begins before an opportunity appears. I could not predict which industries, technologies, or people would become part of my life after release. I could read, write, ask questions, organize information, and build a record that showed how I used my time.

Those habits became transferable. They helped me learn about business, technology, communication, and new communities. They also gave other people something they could examine. A certificate can identify a completed course. A portfolio of work can show how a person thinks, explains, compares, and follows through.

Web3 provides a useful subject for developing those abilities because it combines technology, finance, governance, security, public claims, and human behavior. A learner must separate a problem from a proposed solution, investigate evidence, identify risks, and compare alternatives. Those are valuable habits in many fields, even when a future job has no connection with blockchain.

This lesson examines real-world applications without assuming that blockchain is the best tool for every problem. We will consider recordkeeping, credentials, supply chains, payments, communities, identity, and creative work. We will also examine ordinary databases, signed documents, established payment systems, and trusted intermediaries as possible alternatives.

The independent PP token community gives us a real case. People who did not know me personally learned about the Prison Professors mission, organized independently, and used BNB Smart Chain tools to support the work. The case can inspire careful learning, but it does not promise that another project, token, career plan, or personal story will produce the same response.

I encourage you to keep two questions in view: Does the proposed technology fit the problem, and what useful ability can I demonstrate by evaluating it?

PURPOSE AND ESSENTIAL QUESTION

Lesson 19 evaluates proposed blockchain applications and connects course knowledge with practical abilities that can transfer across industries. It teaches a five-part evaluation sequence and shows how written work can become part of a responsible learning portfolio.

Essential Question:

- » How can I evaluate a proposed blockchain use and document the skills I am developing without treating a career pathway as a promise of employment?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Evaluate applications in recordkeeping, credentials, supply chains, payments, communities, identity, and creative work.
- » Compare a blockchain approach with simpler alternatives such as an ordinary database, signed document, established payment system, or trusted intermediary.
- » Apply the problem, proposed solution, evidence, risks, and alternatives sequence to a hypothetical project.
- » Identify transferable abilities in research, writing, communication, digital safety, project coordination, customer support, compliance awareness, and critical analysis.
- » Distinguish a possible career pathway from a guarantee of employment and describe how a portfolio can document preparation.

KEY TERMS

USE CASE

Definition: A specific problem, task, or process that a technology or service is proposed to address.

Sample sentence: The team defined the use case as verifying course completion across several organizations without exposing a participant's full record.

DIGITAL CREDENTIAL

Definition: A claim represented in digital form and issued by an identified source about a person, organization, object, or achievement.

Sample sentence: The school issued a digital credential stating that the learner completed a course, while the recipient still checked the issuer and credential status.

SUPPLY CHAIN

Definition: The connected people, organizations, processes, goods, and information involved in producing and delivering a product or service.

Sample sentence: The supply chain record followed a component from its manufacturer through transportation, assembly, and final delivery.

COMPLIANCE

Definition: The process of understanding and following applicable laws, regulations, contracts, policies, standards, and organizational requirements.

Sample sentence: The project team asked a qualified professional to review privacy, recordkeeping, and licensing requirements as part of its compliance work.

TRANSFERABLE SKILL

Definition: An ability that can be useful across different jobs, industries, projects, or stages of a career.

Sample sentence: Clear writing is a transferable skill because many roles require a person to explain complex information to other people.

PORTFOLIO

Definition: An organized collection of work that demonstrates knowledge, abilities, progress, and completed projects.

Sample sentence: The learner's portfolio included case analyses, comparison memos, safety checklists, and dated Profile journal entries.

MAIN LESSON

BEGIN WITH THE PROBLEM, NOT THE TECHNOLOGY

A use case begins with a defined problem. A weak proposal often begins with a technology and searches for a reason to use it. A stronger proposal explains who

experiences the problem, what process exists now, what fails, how success will be measured, and which limits must be respected.

Suppose several training organizations want to verify whether a participant completed a course. The problem may involve slow verification, inconsistent records, or dependence on one office. The problem is not simply that the organizations do not use a blockchain. A solution should be judged by whether it improves verification while protecting privacy, correcting errors, controlling access, and managing cost.

A blockchain may help when several parties need a shared, tamper-evident history and no practical recordkeeper is trusted to control every update. It may add unnecessary complexity when one accountable organization can operate a secure database and share verified records through established procedures.

USE FIVE PARTS TO EVALUATE A PROPOSAL

The following sequence organizes the analysis. It can be applied to a blockchain project, a business proposal, a workplace process, or a public claim:

1. Problem: Who experiences the problem? What happens now? Which result needs to improve?
2. Proposed solution: What will the system do? Which people, data, code, organizations, and permissions will it require?
3. Evidence: What working demonstration, documentation, code, audit, agreement, record, user result, or independent review supports the proposal?
4. Risks: What could fail? Who could be harmed? Which privacy, security, financial, operational, legal, accessibility, or governance concerns remain?
5. Alternatives: Could an ordinary database, signed document, established payment system, trusted intermediary, or improved procedure solve the problem more simply?

The sequence does not produce an automatic yes or no. It helps a reviewer explain a conclusion and identify missing information. A proposal may have a legitimate use and still require redesign, safeguards, testing, or a different tool.

RECORDKEEPING ACROSS ORGANIZATIONS

A blockchain can create a shared sequence of records that authorized participants can inspect. Possible uses include tracking approvals, ownership changes, maintenance events, certificates, or transfers. Cryptographic signatures may help show which credential authorized a recorded action.



The record is only as reliable as the process that produces it. If a person enters false information, attaches the wrong document, uses compromised credentials, or records an event that never occurred, a blockchain can preserve the error. The system needs rules for data quality, identity, access, corrections, disputes, and accountability.

An ordinary database may be the stronger choice when one organization has clear responsibility, users need efficient corrections, information must remain private, or the number of participants does not justify a shared network.

DIGITAL CREDENTIALS

A digital credential may represent a course completion, professional license, employment record, membership, identity claim, or other assertion. A useful system identifies the issuer, the subject, the claim, the date, and a way to determine whether the credential remains valid.

The World Wide Web Consortium's Verifiable Credentials Data Model describes an issuer, holder, and verifier relationship. A verifier still decides whether to trust the issuer and whether the credential satisfies the purpose. Digital verification does not guarantee that the original claim was accurate, that the issuer was qualified, or that a credential should be accepted for every use.

Privacy deserves careful attention. Publishing a person's full identity, criminal history, education record, health information, or exact activity on a public ledger could create lasting harm. Many designs keep personal information outside the blockchain and use a limited proof, status record, or cryptographic reference. A signed document or secure verification portal may also serve the need.

SUPPLY-CHAIN TRACEABILITY

A supply chain connects manufacturers, suppliers, transporters, warehouses, retailers, customers, and information systems. A shared ledger may help participants record where an item came from, which organization handled it, when a process occurred, and which documents support the event.

The National Institute of Standards and Technology has examined blockchain and related technologies for manufacturing supply-chain traceability. Its analysis also recognizes the continuing need for accurate data collection, standards, privacy, security, and agreement among participants.

A ledger cannot inspect a physical product by itself. The connection between the record and the product may depend on labels, sensors, inspections, employees, and organizations. If the physical-to-digital link is unreliable, the recorded history may look complete while describing the wrong item or an inaccurate event.

PAYMENTS AND SETTLEMENT

Blockchain networks can transfer digital assets under programmed rules. Possible uses include cross-border transfers, automated distributions, conditional payments, and settlement among organizations. A public record may make selected activity easier to inspect.

A payment use can also introduce volatility, transaction fees, congestion, irreversibility, custody risk, scams, privacy exposure, tax questions, legal requirements, and dependence on conversion services. A stablecoin may reduce one kind of price movement while introducing reserve, issuer, redemption, platform, and regulatory risks.

An established bank transfer, card network, check, money order, or regulated payment service may provide clearer consumer protections, account recovery, dispute procedures, or familiar accounting. The evaluation should compare the complete process rather than one advertised feature.

COMMUNITIES, IDENTITY, AND CREATIVE WORK

Blockchain tools may help a community record membership, distribute access, vote on proposals, manage a treasury, or coordinate contributions. A creator may use a token or non-fungible token to represent access, attribution, a collectible, or a defined right. An identity system may help a person present selected credentials.

The technology does not resolve every human question. A token does not automatically create a legal copyright, a fair royalty, an honest community, or an accurate identity. A public vote may still concentrate influence. A digital item may depend on an outside file, website, marketplace, license, or organization.

Simpler alternatives include membership databases, signed licenses, conventional contracts, access codes, cooperatives, nonprofit governance, and ordinary creative platforms. The preferred approach depends on the problem, participants, evidence, rights, risks, and available safeguards.

WHEN BLOCKCHAIN IS PROBABLY THE WRONG TOOL

A careful analyst should be willing to recommend a non-blockchain solution. Warning signs include:

- » No defined problem or measurable result.
- » One accountable organization already controls the process and can operate a secure database.
- » Sensitive information would be exposed or difficult to correct.
- » Participants cannot verify the source data.

- » The project depends on a token even though the service can work without one.
- » The design adds fees, delays, technical dependencies, or governance conflicts without a clear benefit.
- » A promotional claim replaces a working demonstration, documentation, or independent evidence.
- » Users need recovery, reversibility, customer support, or legal protections that the proposed system does not provide.

Choosing a simpler system is not a rejection of innovation. It shows that the reviewer understands the objective and can compare tools without becoming attached to a label.

APPLIED CASE: AN INDEPENDENT COMMUNITY SUPPORTS PRISON PROFESSORS

The independent PP token community connects the course concepts with a real mission. I first met Changpeng Zhao, known as CZ, while he was going through challenges with the United States justice system. As he prepared for and served four months in federal prison, we communicated frequently. I assisted him as he worked on the manuscript that became *Freedom of Money*, and I later narrated the audiobook.

CZ wrote about his support for Prison Professors and provided resources that help us make educational materials available to people in prison without charge. After the book was released in 2026, people in different parts of the world learned about our mission. A group I did not know formed an independent Web3 community and used the BNB ecosystem to launch a token identified by the symbol PP.

Neither CZ nor I created the token. Prison Professors did not organize, manage, or control the project. The community website identifies the project as independent, not as an official Prison Professors product or endorsement. That separation should remain clear whenever the case is discussed.

DOCUMENTED FACTS

- » The community website describes a PP token operating through smart-contract code on BNB Smart Chain.
- » The website states that a 3 percent transaction charge directs resources toward a public donation address. The website uses the word tax; this course uses transaction charge because the rule comes from code rather than a government.
- » A public blockchain explorer can display the donation address's on-chain balances and transaction history without revealing a private key.
- » A July 21, 2026 snapshot supplied for the approved Lesson 9 showed the public address holding more than 943 WBNB and a smaller native BNB



balance. The community's Telegram tracker reported more than 943 BNB in cumulative donations at approximately the same time.

- » The balance snapshot and community running total describe related activity in different ways. Both can change, and any dollar estimate changes with the market price of BNB.

MY PERSPECTIVE AND FUTURE GOAL

I see the community's work as evidence that a documented mission can reach people who do not know the founder personally. The organizers could read about our work, examine the record, and decide whether they wanted to help. Their response does not guarantee that another learner's writing will attract an employer, mentor, investor, or supporter. It shows why a sustained body of work gives other people something meaningful to evaluate.

I have described the treasury arrangement as cold storage and pledged to reserve the resources at least until summer 2027 while we build a responsible, mission-aligned plan. I have also connected future use with reaching meaningful participation in Prison Professors programs. Those are stated goals and commitments. Future decisions still require policies, custody controls, accounting, governance, reporting, and human accountability.

RESULTS AND LIMITATIONS

The case shows that people across borders can use a network, smart contract, token, communication channel, and public address to coordinate support. It also shows that a blockchain record can help an observer verify selected balances and transactions instead of relying only on a private report.

The public ledger does not prove why every transfer occurred, who controls every connected account, how signing credentials are stored, whether a future promise will be honored, how resources will be used, what legal or accounting treatment applies, or what any token will be worth later. The token, independent community, public treasury, market activity, and Prison Professors stewardship are connected but distinct parts of the system.

The case does not establish that PP, BNB, WBNB, or any other asset is safe, liquid, suitable, or legally classified in a particular way. It does not recommend an asset or predict a return. A complete evaluation should compare the community approach with direct donations, grants, conventional payment services, memberships, and other ways of supporting a mission.

THE CASE REVEALS TRANSFERABLE ABILITIES

A learner can study the PP community case without owning a token or using a wallet. The analysis itself can demonstrate useful abilities:

- » Research: Locate and compare the community website, public ledger, organizational statements, and dated source records.
- » Critical analysis: Separate documented facts, first-person perspective, observed results, future goals, promotional claims, and unresolved questions.
- » Writing: Explain technical concepts in plain language and organize a conclusion around evidence.
- » Digital safety: Distinguish a public address from a private key and identify impersonation, custody, and privacy risks.
- » Project coordination: Identify roles, dependencies, decisions, milestones, reporting needs, and alternative approaches.
- » Customer or community support: Anticipate questions from learners, donors, community members, and people unfamiliar with Web3.
- » Compliance awareness: Recognize when privacy, nonprofit accounting, tax, licensing, consumer protection, or other qualified review may be needed.
- » Communication: Describe both possible benefits and unresolved risks without using hype or dismissive language.

A CAREER PATHWAY IS NOT AN EMPLOYMENT PROMISE

Web3 organizations and adjacent technology companies may need software developers, security specialists, data analysts, researchers, technical writers, customer-support staff, community moderators, project coordinators, product staff, policy researchers, compliance personnel, and operations teams. The same abilities can apply in finance, education, government, manufacturing, logistics, nonprofit work, and other fields.

A course does not qualify a person for every role. Some positions require formal education, certifications, professional licenses, programming experience, background checks, unrestricted technology access, or specialized knowledge. Employer needs and legal requirements can change. A criminal record may affect eligibility differently across employers, jobs, industries, and jurisdictions.

A responsible career statement uses evidence. Instead of writing, “I completed one course, so I am ready to become a blockchain analyst,” a learner might write, “I completed a 20-lesson course, developed a working vocabulary, analyzed several cases, compared risks and alternatives, and created written samples that show my current abilities. My next step is to strengthen research, writing, spreadsheet, security, or programming skills according to the pathway I choose.”



BUILD A PORTFOLIO BEFORE YOU NEED IT

A portfolio converts a general claim into work another person can review. A Profile journal can become one part of that portfolio. The strongest collection is organized, dated, honest about current ability, and updated as skills improve.

POSSIBLE OFFLINE PORTFOLIO ITEMS INCLUDE:

- » A glossary that explains technical terms in original language.
- » A one-page comparison of a blockchain solution and a conventional alternative.
- » A case brief separating facts, claims, evidence, risks, and unanswered questions.
- » A transaction or governance safety checklist.
- » A written response to a fictional customer-support question.
- » A project outline identifying objectives, roles, dependencies, milestones, and reporting.
- » A research log showing source, date, claim, supporting evidence, and uncertainty.
- » A continuing-learning plan that identifies the next skill, study resource, practice activity, and evidence of completion.

Do not include confidential records, credentials, private keys, seed phrases, account numbers, real wallet addresses, or another person's personal information. A portfolio should demonstrate judgment as well as knowledge.

COMPLIANCE AND ETHICS SUPPORT RESPONSIBLE WORK

Compliance awareness begins by recognizing that a technical feature may operate inside legal, contractual, organizational, and professional requirements. Payments, identity, credentials, securities, taxes, privacy, consumer protection, nonprofit accounting, record retention, intellectual property, and sanctions can involve different rules. The facts and jurisdiction determine which requirements apply.

A beginner does not need to provide a legal conclusion. A useful contribution may be to identify the question, preserve the source, document uncertainty, and refer the issue to a qualified person. Ethical work also requires honest communication, respect for privacy, protection of credentials, accurate reporting, conflict disclosure, and a willingness to correct errors.

Responsible preparation means knowing the boundary of your current knowledge. That habit builds credibility because it replaces confident guessing with a documented process.



APPLIED SCENARIO: THE PATHWAYPASS CREDENTIAL PROPOSAL

This scenario is fictional. It does not describe an existing Prison Professors product, facility system, credential, blockchain, or employer arrangement.

A nonprofit called Pathway Learning works with prisons, reentry organizations, and employers. Participants currently receive paper course certificates. Verification can take several weeks because records remain in separate offices. Some certificates have been lost, and some employers do not know whom to contact.

A vendor proposes PathwayPass, a public-blockchain credential system. Each course completion would create a permanent public record linked to a participant identifier. The vendor says employers could verify completion without calling the nonprofit. The proposal also includes a token that facilities would purchase to issue credentials.

The presentation uses the phrases tamper-proof, lifetime identity, and guaranteed employer trust. It does not explain how incorrect records would be corrected, how a credential would be revoked, how participants would consent, who could connect an identifier with a name, what happens when a private key is lost, why a token is required, or how facilities without reliable internet access would participate.

A staff member proposes an alternative: keep the records in the nonprofit's secure database, issue a digitally signed certificate, and provide employers with a verification phone number and limited online portal. The alternative would not create a public ledger, but it would allow corrections, revocation, account recovery, and one accountable recordkeeper.

SCENARIO QUESTIONS

1. Define the problem without assuming that either proposal is the solution.
2. Describe the proposed blockchain solution, including the participants, data, identifier, credential, token, network, keys, and verification process.
3. Identify at least six pieces of evidence or missing information needed before accepting the vendor's claims.
4. Identify privacy, security, accuracy, access, correction, recovery, cost, governance, legal, and operational risks.
5. Compare PathwayPass with the signed-certificate and verification-portal alternative. Which conditions could favor each approach?
6. Recommend a limited pilot or next research step. Explain what should be tested, what information should remain private, and how participant consent and error correction should work.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- » Shared records may reduce reconciliation among organizations.
- » Digital signatures and tamper-evident history may support verification.
- » Smart contracts may automate defined distributions or approvals.
- » Public records may improve selected forms of transparency.
- » Portable credentials may help a person present verified claims across services.
- » Open networks may help communities coordinate across borders.
- » Studying the systems can develop research, writing, safety, and analytical abilities.

LIMITATIONS AND RISKS

- » Incorrect source data can become a durable incorrect record.
- » Public records may create privacy, targeting, or discrimination risks.
- » Keys, interfaces, or administrators may create control and recovery failures.
- » Smart-contract defects, oracle failures, or upgrades may change outcomes.
- » Tokens may add volatility, liquidity, custody, fraud, and legal exposure.
- » Organizations may disagree about standards, authority, corrections, or responsibility.
- » A blockchain may cost more and perform less efficiently than a conventional system.
- » Job requirements, technology, and legal obligations can change.
- » A course, credential, portfolio, or community connection does not guarantee employment or financial success.

COMMON MISCONCEPTIONS

- » “If the record is on a blockchain, the original information must be true.”
- » “A digital credential proves that every verifier must accept the claim.”
- » “A token is necessary for every blockchain application.”
- » “A public ledger provides complete transparency about people, purpose, custody, and future decisions.”
- » “Decentralized means no person or organization has influence.”
- » “Completing a Web3 course guarantees a Web3 job.”
- » “A portfolio should hide uncertainty and present the learner as an expert.”
- » “Recommending a conventional solution shows a lack of technical knowledge.”



OFFLINE EXERCISE: EVALUATE A PROPOSED PROJECT

Materials: Separate paper and a pen or pencil. Use the PathwayPass scenario or choose another fictional project described in this lesson. You do not need internet access, an account, a wallet, a digital asset, or a transaction.

Create five labeled sections and complete each one:

1. **Problem:** Write two or three sentences identifying the people, current process, failure, and desired result.
2. **Proposed solution:** Describe the technical and human components. Include data sources, permissions, control points, and dependencies.
3. **Evidence:** List at least five items that would help you test whether the proposal works as described.
4. **Risks:** Identify at least eight concerns across privacy, security, accuracy, cost, access, operations, governance, financial exposure, and legal uncertainty.
5. **Alternatives:** Compare at least two non-blockchain approaches. State which facts would help you choose among the options.

Finish with a six- to eight-sentence recommendation. You may recommend proceeding, rejecting the proposal, conducting a limited pilot, redesigning the system, or gathering more evidence. Support the recommendation with facts and identify at least one uncertainty.

Portfolio extension: Save the dated worksheet when circumstances permit. Add a short note identifying the abilities the work demonstrates, such as research planning, critical analysis, risk identification, clear writing, or project evaluation.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which question should come first when evaluating a proposed blockchain use?
 - a. What token will the project sell?
 - b. What defined problem needs to be solved, and who experiences it?
 - c. Which network has the most advertising?
 - d. How quickly can the project promise a return?
2. Which statement best describes a digital credential?
 - a. A digital claim from an identified issuer that still requires evaluation of the issuer, claim, status, and purpose



- b. A public record that every employer must accept
 - c. A guarantee that the original information was correct
 - d. A token that always has a market price
- 3. Which example best demonstrates a transferable skill?
 - a. Repeating a project's promotional slogan
 - b. Claiming expert status after one course
 - c. Writing a clear comparison of evidence, risks, and alternatives that another person can review
 - d. Purchasing a token to prove interest in technology

TRUE OR FALSE

- » If a blockchain can preserve a record against later alteration, the blockchain also guarantees that the original information was accurate and that no correction process is needed.

SHORT EXPLANATION

- » In four to six sentences, explain how a person can use a Web3 case analysis to demonstrate transferable abilities without claiming that a course or portfolio guarantees employment.

SUMMARY AND PRACTICAL TAKEAWAYS

- » A use case identifies a specific problem, task, or process.
- » A disciplined evaluation examines the problem, proposed solution, evidence, risks, and alternatives.
- » Blockchain can support shared records, credentials, supply-chain events, payments, communities, identity claims, and creative applications.
- » A ledger preserves recorded data; it does not guarantee that source data, identity, rights, or claims are accurate.
- » Ordinary databases, signed documents, established payment systems, trusted intermediaries, and improved procedures may offer simpler solutions.
- » The independent PP token community shows how a global group used BNB Smart Chain tools to support a mission while remaining separate from Prison Professors.
- » The PP case includes documented facts, personal perspective, observed results, future goals, and unanswered questions that should not be blended together.



- » Research, writing, communication, digital safety, project coordination, customer support, compliance awareness, and critical analysis are transferable abilities.
- » A portfolio can document current abilities through dated work samples and honest explanations.
- » A career pathway describes preparation and next steps; it does not promise a job, income, acceptance, or future success.

The practical takeaway is to become a careful evaluator and a disciplined documenter. You do not need to own a digital asset to show that you can learn a complex subject, compare systems, communicate clearly, identify uncertainty, and prepare for future responsibility.

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:

- » Describe one real-world use that you understand more clearly after completing this lesson.
- » Apply the problem, proposed solution, evidence, risks, and alternatives sequence to that use.
- » Explain when a blockchain approach may help and when a simpler system may be stronger.
- » Identify at least three transferable abilities you have practiced through this course.
- » Describe one work sample you could preserve in a portfolio and what it would demonstrate.
- » Use the independent PP token community case to explain how documented work can become visible to people who do not yet know you.
- » Explain why the community case does not guarantee that your work will produce the same response or that a Web3 course will lead to employment.
- » State one realistic next step for developing and documenting a skill that could support your future.

Your response should show honest self-assessment and practical planning. You are not being asked to purchase an asset, create an account, open a wallet, join a community, disclose private information, or conduct a transaction.



SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 19: Real-World Applications, Limitations, and Career Skills, and the date you completed the entry.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 19 — [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 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, employer confidential information, or another person's sensitive information.

UNDERSTANDING WEB3

LESSON 20: PREPARING RESPONSIBLY FOR THE FUTURE OF WEB3

A Prison Professors Self-Directed Course

Estimated time: 90–125 minutes

Educational and Safety Boundary:

This lesson provides general education about Web3, ethics, uncertainty, continuing education, career preparation, and related risks. It does not provide individualized financial, investment, legal, tax, employment, or career advice. No activity requires internet access, an account, a wallet, a digital asset, a purchase, or a transaction.

Opening Guidance

During 26 years in federal prison, I learned to prepare for a future I could not see. I did not know which technologies would exist when I returned to society. I did know that I could read, write, ask questions, organize information, and create a record of disciplined effort. Those choices gave me a constructive response to uncertainty.

I pursued self-directed learning because I expected limits on employment after release. I wanted to develop skills that could help me create opportunities and multiple income streams. I also wanted other people to see how I used my time. Dated writing, completed projects, correspondence, and a record of follow-through helped people evaluate my preparation before they knew me well.

The internet changed substantially while I was incarcerated, and it continued changing after my release. Blockchain, digital assets, smart contracts, decentralized finance, and new forms of online coordination became part of that change. I did not need to predict every development. I needed a process for learning, checking claims, protecting myself, and deciding which abilities to develop.

That process remains useful. Web3 includes working systems, active experiments, unfinished standards, promotional claims, and forecasts that may never become reality. A responsible learner does not treat all of those categories as equal. The learner identifies what can be observed now, what is still being tested, what is only predicted, and which evidence could change the conclusion.

This final lesson brings the course together. Completion does not make a person an expert, promise a job, or require financial participation. It gives you a foundation for continuing to learn. I encourage you to finish with a written plan and a capstone that another person can review. The quality of that work can show judgment, persistence, communication, and personal responsibility.

PURPOSE AND ESSENTIAL QUESTION

Lesson 20 synthesizes the course, examines uncertainty, and helps you create a realistic continuing-learning plan. It separates established capabilities from work in progress and future forecasts. It also connects responsible innovation with ethics, safety, evidence, accountability, and practical preparation.

Essential Question:

- » How can I use what I learned about Web3 to evaluate future claims, continue developing useful skills, and document a responsible plan without purchasing an asset or creating an account?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- » Summarize the course's major concepts and recurring risks.
- » Distinguish established capabilities from forecasts about the future.
- » Identify lawful and ethical ways to continue learning without purchasing assets or creating accounts.
- » Create a personal plan for skill development, evidence of preparation, and responsible participation.

KEY TERMS

RESPONSIBLE INNOVATION

Definition: The development, use, or evaluation of technology with attention to purpose, evidence, people affected, safety, fairness, privacy, accountability, access, and long-term consequences.

Sample sentence: The team practiced responsible innovation by testing the claimed benefit, protecting private data, identifying who could be harmed, and assigning authority for corrections.

ETHICS

Definition: Principles and reasoning used to evaluate right conduct, duties, harms, fairness, honesty, and responsibility.

Sample sentence: Ethics led the analyst to ask whether a legal data practice was also fair to people who could not correct an inaccurate record.



UNCERTAINTY

Definition: A condition in which available knowledge is incomplete, changing, or insufficient for a guaranteed conclusion.

Sample sentence: The proposal acknowledged uncertainty about future adoption instead of presenting a pilot as a universal solution.

CONTINUING EDUCATION

Definition: Intentional learning that continues after a course through study, practice, feedback, reflection, and updated evidence.

Sample sentence: My continuing education plan combines reading, written summaries, case analysis, and monthly review.

ACTION PLAN

Definition: A written sequence that identifies an objective, tasks, resources, dates, evidence of completion, and a point for review or adjustment.

Sample sentence: The action plan divides one learning goal into 30-, 60-, and 90-day stages.

EVIDENCE OF PREPARATION

Definition: Dated, reviewable work that shows knowledge, skill, effort, reliability, and improvement.

Sample sentence: The learner used revised case briefs, a safety checklist, and Profile journal entries as evidence of preparation.

MAIN LESSON

A MAP OF THE COURSE

The course developed through six connected areas. Each area answered a different part of the larger question: What is Web3, how does it work, where can it help, and how can a person participate responsibly?

- » Section 1 — Internet and Web3 foundations: self-directed learning, changes from the early web to Web2 and Web3, ownership and participation claims, centralization, decentralization, and tradeoffs.
- » Section 2 — Blockchain foundations: blocks, transactions, hashes, nodes, networks, consensus, network comparisons, and layers.

- » Section 3 — Digital assets and tokenization: cryptocurrencies, coins, tokens, stablecoins, tokenization, non-fungible tokens, uses, structures, limitations, and risks.
- » Section 4 — Access and safety: wallets, public addresses, private keys, seed phrases, custody, self-custody, transaction flow, scams, privacy, and irreversible errors.
- » Section 5 — Programmed applications and coordination: smart contracts, decentralized applications, oracles, decentralized finance, decentralized organizations, governance, treasuries, voting power, and accountability.
- » Section 6 — Application and preparation: real-world uses, conventional alternatives, transferable skills, career pathways, future claims, ethical participation, and a continuing-learning plan.

The sections build a connected way of thinking. A token depends on a network. A wallet or service helps a person interact with that network. A smart contract may define rules. An application may provide an interface. Governance may change the rules. Oracles or administrators may add outside information and human control. Every layer creates questions about authority, security, access, evidence, and responsibility.

SEVEN RECURRING QUESTIONS

A changing technology becomes easier to evaluate when the learner returns to a durable set of questions. These questions apply to a blockchain project, a workplace proposal, a financial claim, an online community, or a forecast:

- » What problem is being described, and who experiences it?
- » How does the proposed system work in technical and human terms?
- » Who can control, change, pause, upgrade, approve, reverse, or influence an outcome?
- » Which claim is supported by observable evidence, and what remains unverified?
- » Which security, privacy, financial, legal, operational, access, and governance risks remain?
- » Could a simpler or more familiar system achieve the objective?
- » Who is accountable when the system fails, harms someone, or produces an incorrect result?

These questions reduce dependence on slogans. They also help a beginner contribute without pretending to know everything. A clear question, supported by a source and a dated note, can be a valuable form of work.



SEPARATE THE PRESENT FROM THE POSSIBLE FUTURE

Future discussions often combine three different categories. A careful explanation separates them and dates the supporting evidence.

Established or currently observable capability: A system, feature, standard, or event can be examined now through operating code, official documentation, a published standard, a public record, a completed transaction, or another reliable source. Public blockchains can record and validate transactions under network rules. Smart contracts can execute programmed instructions. A public explorer can display selected on-chain records. These capabilities do not prove that every use is safe, accurate, fair, legal, or suitable.

Active development, pilot, or working draft: A design is being tested, revised, standardized, or used on a limited basis. The work can be real without being final or widely adopted. For example, the World Wide Web Consortium published the Verifiable Credentials Data Model v2.0 as a Recommendation in 2025. In May 2026, version 2.1 was a Working Draft. The draft status tells a reader that the newer text may change and should not be described as a final standard.

Forecast, expectation, or speculation: A statement describes what someone believes may happen later. Examples include predictions that every employer will use blockchain credentials, every bank will move all activity on-chain, a token will reach a certain price, or a particular job category will expand by a precise amount. A forecast may be informed or uninformed, but it is not a present fact.

A claim can move from one category to another as evidence changes. A working draft can become an approved standard. A pilot can become a larger service or be discontinued. A forecast can receive support, remain unresolved, or prove false. Dating the source helps another reader understand what was known when the statement was written.

USE AN EVIDENCE LADDER

Not all support has the same strength. A learner can organize evidence from weaker to stronger without assuming that one item settles every question:

- » An anonymous post, advertisement, slogan, or repeated rumor.
- » A named person's opinion, estimate, or prediction.
- » A project website, white paper, or official statement describing its own design.
- » Technical documentation, source code, public records, or a reproducible demonstration.
- » A completed pilot with disclosed methods, limits, and results.

- » An independent audit, evaluation, peer-reviewed study, regulator record, or adopted standard.
- » Continued performance observed across time, conditions, and different users.

The ladder does not eliminate judgment. A project website may accurately describe code while presenting benefits more confidently than risks. An audit may cover only a defined version or component. A public record may show a transaction without explaining identity, intent, custody, off-chain agreements, or future decisions. Strong analysis states what each source supports and what it cannot establish.

UNCERTAINTY IS PART OF RESPONSIBLE ANALYSIS

Technology, law, standards, prices, providers, security conditions, and public behavior can change. A responsible explanation does not hide that uncertainty. It describes the current evidence, the limits of the evidence, and the facts that would justify an updated conclusion.

Uncertainty should not become an excuse for careless claims or total inaction. A learner can still take useful steps: protect credentials, avoid urgency, compare sources, use hypothetical amounts, preserve dated notes, ask qualified professionals when necessary, and choose learning activities that do not create financial exposure.

The Commodity Futures Trading Commission warns that virtual-currency markets can involve volatility, fraud, cyber risk, limited customer protections, and uncertain future value. Those warnings support caution. They do not tell every person what decision to make, and this course does not provide an individual recommendation.

RESPONSIBLE INNOVATION BEGINS WITH PEOPLE AND PURPOSE

A new technical feature can attract attention before anyone defines the human objective. Responsible innovation reverses that order. It begins with the problem, the people affected, and the result that the team is trying to improve.

A responsible-innovation review can include the following questions:

- » Purpose: Which defined problem is the project trying to solve?
- » People: Who benefits, who carries risk, and who may be excluded?
- » Evidence: Which current facts support the proposed design or expected result?
- » Safety: How will the project address security, privacy, recovery, errors, abuse, and fraud?
- » Fairness: Can affected people understand the process, give meaningful consent, and challenge a decision?



- » Access: Does the system create barriers based on money, devices, literacy, disability, location, or incarceration?
- » Governance: Who sets rules, controls resources, resolves conflicts, and authorizes changes?
- » Alternatives: Could a simpler database, contract, institution, or procedure produce a stronger result?
- » Review: How will the team measure results, report failures, receive feedback, and correct course?

A design can be technically impressive and still fail this review. Code cannot decide whether the purpose is fair, whether an exclusion is acceptable, or whether a community has earned trust. People remain responsible for those decisions.

ETHICS EXTENDS BEYOND MINIMUM COMPLIANCE

Laws, regulations, contracts, institutional rules, and professional standards create important boundaries. Compliance asks whether a person or organization follows applicable requirements. Ethics asks additional questions about honesty, fairness, harm, duty, dignity, and stewardship.

A data practice may be technically permitted yet expose more personal information than the service needs. A token distribution may follow code yet concentrate influence in a small group. A marketing statement may avoid a direct falsehood yet create a misleading impression through omitted risks. An ethical review examines those consequences.

A beginner should not invent a legal conclusion. A responsible response may identify the issue, preserve the source, describe the uncertainty, follow facility and organizational rules, and refer a specialized question to a qualified professional.

THE PRISON PROFESSORS CASE: RECORDS, COMMITMENTS, AND FORECASTS

The independent PP token community offers a practical way to apply these categories. After the publication of Freedom of Money in 2026, people unknown to CZ and me organized an independent token community connected with the Prison Professors mission. Neither CZ nor I created the token, and Prison Professors did not organize, manage, or control the project.

The community website, smart-contract records, public treasury address, and dated blockchain-explorer snapshot provide evidence that can be examined. In Lesson 9, we provided a snapshot from July 21, 2026, which showed the public address holding more than 943 WBNB and a smaller native BNB balance. The figure was a dated observation, not a permanent value.

I described the treasury arrangement as cold storage and pledged to reserve the resources at least until summer 2027 while we develop a responsible, mission-aligned plan. That statement records my commitment. It does not establish future value, legal or tax treatment, custody details, community participation, mission results, or the final use of resources. Those questions require continuing documentation and appropriate review.

The case also shows why documented work can reach people who do not know the author personally. The community could read about our mission and examine a body of work. I find that response encouraging, but I do not present it as a formula or promise. Another learner's work may create a different opportunity, or it may not receive immediate attention. The responsible lesson is to build credible evidence before an opportunity appears.

CONTINUE LEARNING WITHOUT BUYING ANYTHING

A person can develop Web3 knowledge without purchasing an asset, opening an account, using a wallet, or accessing a live application. The learning objective is not financial participation. It is stronger understanding and better judgment.

- » Review the course glossary and rewrite definitions in your own language.
- » Read approved books, newspapers, magazines, course materials, or institutional resources.
- » Use correspondence to ask a teacher, librarian, mentor, family member, or professional a focused question.
- » Write a one-page explanation of a concept for a person who has not studied Web3.
- » Compare a blockchain proposal with a conventional alternative.
- » Analyze a fictional transaction, governance proposal, scam message, or credential system.
- » Keep a dated question log and record which source answered each question.
- » Revise earlier work after receiving feedback, and explain what changed.
- » Create safety, source-evaluation, and project-review checklists.
- » Preserve Profile journal entries and other work samples when facility rules permit.

If internet access becomes available later, the same habits still apply. Use primary and official sources when possible. Check the publication date and status. Distinguish documentation from advertising. Never enter a private key, seed phrase, password, authentication code, or confidential information into an unfamiliar site or message.

PRACTICE INFORMATION HYGIENE

Information hygiene is the routine of keeping sources, claims, and uncertainty organized. It can reduce confusion when a subject changes quickly.

- » Record the source title, author or organization, publication date, and date reviewed.
- » Label the source as official documentation, adopted standard, working draft, research, news, opinion, promotion, or personal account.
- » Write the exact claim in your own language and identify the supporting evidence.
- » Separate current fact, personal perspective, observed result, commitment, and forecast.
- » Record what the source does not prove and which questions remain open.
- » Return to time-sensitive notes before publication, instruction, or a major decision.

This practice supports clear writing. It also makes revision easier because the learner can identify which conclusion depends on a changing source.

BUILD EVIDENCE OF PREPARATION

A certificate can show that a person completed a course. Evidence of preparation shows what the person can explain, analyze, create, revise, and complete. A useful collection may include:

- » A dated glossary with original definitions and sample sentences.
- » A comparison memo evaluating a blockchain design and a conventional alternative.
- » A case brief separating facts, claims, evidence, risks, commitments, forecasts, and open questions.
- » A wallet, transaction, privacy, or scam-prevention checklist.
- » A fictional customer-support response that explains a technical problem clearly and safely.
- » A project outline with objectives, roles, dependencies, milestones, and reporting.
- » A revised work sample accompanied by a short explanation of the feedback used.
- » A 30-, 60-, and 90-day action plan.
- » The final Profile capstone from this lesson.



The collection should represent current ability honestly. Do not include private keys, seed phrases, passwords, authentication codes, account numbers, real wallet addresses, another person's private information, employer confidential information, or facility-sensitive information. Replace sensitive details with clearly labeled fictional examples.

RESPONSIBLE PARTICIPATION IS A PATTERN OF CONDUCT

Responsible participation does not begin with a transaction. It begins with conduct. A person can practice the following habits in study, work, community service, business, and technology:

- » Slow down when a message creates urgency, fear, secrecy, or pressure.
- » State uncertainty instead of presenting a guess as a fact.
- » Disclose conflicts, incentives, control, and important limitations.
- » Respect privacy, consent, intellectual property, contracts, and institutional rules.
- » Use only access and information that you are authorized to use.
- » Protect credentials and verify addresses, identities, instructions, and counterparties.
- » Document decisions, corrections, failures, and lessons learned.
- » Seek qualified help for legal, tax, financial, security, health, or other specialized questions.
- » Avoid promises of profit, guaranteed adoption, employment, support, or personal outcomes.

These habits are useful beyond Web3. They help a person earn credibility because other people can see a consistent process rather than a confident slogan.

AN ACTION PLAN CONVERTS INTEREST INTO PRACTICE

A general intention such as “learn more about blockchain” is difficult to measure. An action plan defines a narrow objective, available resources, tasks, dates, evidence, and a review point.

A realistic plan fits current conditions. An incarcerated learner may depend on books, printed materials, correspondence, classes, approved institutional messaging, and handwritten work. A released learner may have additional tools. Neither person needs to pretend that unavailable resources are available.

A plan should also allow adjustment. If a resource does not arrive, select another approved source. If a concept remains unclear, return to the foundation and write a



new explanation. If feedback reveals an error, revise the work and preserve both the original date and the revision date. Adjustment is evidence of learning, not failure.

APPLIED SCENARIO: THE FUTUREREADY WEB3 FORECAST

This scenario is fictional. It does not describe an existing Prison Professors course, employer, token, credential, investment, or partnership.

A magazine article promotes a program called FutureReady Web3. The article states that within two years every employer will verify education through block-chain credentials, every major bank will move all customer activity on-chain, artificial-intelligence agents will conduct most transactions, and the program's token will increase ten times in price.

The article says that anyone who finishes its six-week course is guaranteed a Web3 job. It cites a limited credential pilot at three organizations as proof of universal adoption. It also cites the World Wide Web Consortium's Verifiable Credentials Data Model v2.1 as a final global standard, even though the cited document is labeled Working Draft.

The article provides no audited employment results, no method for its price prediction, no explanation of employer requirements, no security review, and no comparison with signed digital credentials or ordinary databases. Enrollment requires an immediate token purchase. A countdown clock says that hesitation will eliminate the opportunity.

SCENARIO QUESTIONS

- » Classify each major statement as an established or currently observable capability, active development or pilot, forecast, or unsupported promotional claim.
- » Identify at least eight pieces of evidence or missing information that a responsible reviewer would seek.
- » Explain why a three-organization pilot does not establish universal adoption and why a Working Draft should not be described as a final standard.
- » Identify financial, security, privacy, employment, access, governance, and ethical concerns in the offer.
- » Rewrite two of the article's claims using accurate categories, dates, limitations, and uncertainty.
- » Recommend one continuing-learning activity that does not require a token purchase, account, wallet, or internet connection.



BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS OF CONTINUED WEB3 STUDY

- » A learner can understand technology that may influence finance, identity, organizations, records, and creative work.
- » Case analysis can strengthen research, writing, source evaluation, communication, and critical thinking.
- » Safety education can help a person recognize impersonation, credential theft, false urgency, and irreversible errors.
- » Comparing blockchain with conventional systems can improve project and business judgment.
- » Dated work samples can show preparation, revision, persistence, and ethical reasoning.
- » Continuing education can help a learner adapt when technology, standards, and workplace needs change.

LIMITATIONS AND RISKS

- » Course concepts and examples can become outdated.
- » Restricted access may prevent direct use of devices, networks, applications, or current sources.
- » Promotional material may present forecasts as present facts.
- » Public records may be accurate about recorded events yet incomplete about identity, intent, custody, or off-chain activity.
- » Digital assets may involve volatility, liquidity limits, fraud, custody failures, cyber risk, fees, and legal uncertainty.
- » Smart contracts, interfaces, oracles, administrators, and governance systems may fail or be exploited.
- » Public or permanent records may create privacy, correction, discrimination, or safety concerns.
- » Standards, laws, employers, providers, and community practices can change.
- » A course, certificate, Profile, portfolio, relationship, or plan cannot guarantee income, employment, adoption, support, or release outcomes.

COMMON MISCONCEPTIONS

- » “A prediction from a famous person is an established fact.”
- » “A pilot proves that every organization will adopt the system.”



- » “A Working Draft is the same as a final standard.”
- » “Responsible innovation means using the newest technology available.”
- » “If an action is technically possible or legally permitted, it is automatically ethical.”
- » “A public blockchain reveals every fact about a project and every person involved.”
- » “Continuing education requires buying an asset or opening an account.”
- » “Completing this course makes a learner a Web3 expert.”
- » “A portfolio should hide mistakes and uncertainty.”
- » “A 90-day plan guarantees an opportunity at the end of 90 days.”

OFFLINE EXERCISE: BUILD A 30-, 60-, AND 90-DAY LEARNING PLAN

Materials: Separate paper and a pen or pencil. You may use this workbook, approved books, correspondence, classes, writing exercises, or other institutional resources. You do not need internet access, an account, a wallet, a digital asset, a purchase, or a transaction.

STEP 1: CHOOSE ONE OBJECTIVE

Write one objective that can be demonstrated. Examples include explaining blockchain in plain language, evaluating Web3 claims, improving technical writing, building a safety checklist, comparing governance systems, or creating a project-analysis portfolio. Do not write a promised result that another person controls.

STEP 2: DEFINE THE 30-DAY FOUNDATION

- » Identify two available learning resources.
- » Review or create a glossary of at least 20 course terms.
- » Produce one baseline work sample that shows your current understanding.
- » Write three questions you want the next stage to answer.
- » Record a review date and the evidence you will preserve.

STEP 3: DEFINE THE 60-DAY PRACTICE STAGE

- » Create two or three additional work samples.
- » Use at least one comparison, scenario, or source-evaluation exercise.
- » Seek feedback through an approved teacher, mentor, family member, class, or correspondence method when available.
- » Revise one work sample and explain what changed.
- » Update the question log and source record.



STEP 4: DEFINE THE 90-DAY EVIDENCE STAGE

- » Complete the final Profile capstone in this lesson.
- » Organize selected work into a dated list or portfolio record.
- » Write a short statement describing the abilities the work demonstrates.
- » Identify one limitation in your current knowledge and the next resource you need.
- » Set the next review date and a new learning objective.

STEP 5: TEST THE PLAN

Review the complete plan and answer the following questions:

- » Can I complete each task with the resources and permissions available to me?
- » Does each stage produce evidence that another person could review?
- » Have I avoided financial participation, sensitive information, unauthorized access, and unrealistic promises?
- » Does the plan include dates, feedback, revision, and a decision point?
- » What alternative will I use if a resource or opportunity is unavailable?

Keep the plan with your course work when circumstances permit. Record the date you complete each stage. If conditions change, revise the plan and explain the reason.

KNOWLEDGE CHECK

MULTIPLE CHOICE

Which statement best describes an established or currently observable capability?

- a. A claim that every employer will use blockchain credentials within two years
- b. A public blockchain currently records transactions under its network rules
- c. A prediction that one token will increase ten times in price
- d. A promise that one course will guarantee employment

Which action best demonstrates responsible innovation?

- a. Selecting a blockchain before defining the problem
- b. Removing risk disclosures so users remain enthusiastic
- c. Examining purpose, evidence, affected people, safeguards, access, governance, and alternatives
- d. Assuming that legal permission resolves every ethical question



Which example is strongest as evidence of preparation?

- a. A general claim that the learner is passionate about technology
- b. A token purchase made to show interest
- c. A dated set of original work samples showing analysis, feedback, revision, and completion
- d. A copied promotional description of a project

TRUE OR FALSE

- » A forecast becomes an established fact when a confident or well-known person repeats it.

SHORT EXPLANATION

- » In four to six sentences, explain the difference between an established capability and a forecast. Give one example of each and identify one piece of evidence that could support an updated conclusion.

SUMMARY AND PRACTICAL TAKEAWAYS

- » Web3 combines networks, digital assets, wallets, smart contracts, applications, organizations, and human decisions.
- » The course's recurring risks include security failures, privacy exposure, scams, volatility, custody loss, irreversible errors, concentrated control, unclear accountability, and legal uncertainty.
- » An established capability can be observed now; a pilot or working draft remains in development; a forecast describes a possible future.
- » A source should be dated, categorized, and limited to the claim it actually supports.
- » Responsible innovation examines purpose, people, evidence, safety, fairness, access, governance, alternatives, and correction.
- » Ethical judgment includes honesty, dignity, harm, duty, fairness, and stewardship, even when a technical action is possible.
- » The independent PP token community provides a case for separating public records, personal perspective, commitments, observed results, forecasts, and unanswered questions.
- » Continuing education can rely on reading, writing, correspondence, classes, comparison, scenario analysis, feedback, and revision.



- » Evidence of preparation consists of dated, reviewable work that represents current ability honestly.
- » A 30-, 60-, and 90-day action plan converts a broad intention into tasks, evidence, dates, review, and adjustment.
- » No course, certificate, plan, Profile, portfolio, relationship, or Web3 project can guarantee a job, income, support, adoption, or personal outcome.

The practical takeaway is to keep learning with discipline. Separate present evidence from future possibility, protect yourself and other people, document your work, revise when facts change, and build a record that shows how you think and follow through.

FINAL PROFILE CAPSTONE ASSIGNMENT

Title: What I Learned About Web3 and How I Am Preparing for the Future

Length: 800–1,200 words

Write one coherent essay in a personal, first-person voice. Organize the response with an introduction, connected body paragraphs, and a conclusion. Do not submit a disconnected list of answers. Use the prompts below to guide your writing:

- » Explain why you chose to complete the course and how self-directed learning connects with your future.
- » Summarize blockchain, Web3, digital assets, wallets, smart contracts, decentralized applications, decentralized finance, and governance in your own language.
- » Identify at least four recurring risks or limitations and explain how a responsible participant responds.
- » Describe the difference among an established capability, active development or pilot, and a forecast. Provide one example of each.
- » Use the independent PP token community case to separate a public record, a personal perspective, an observed result, a commitment, a forecast, and an unanswered question.
- » Explain what responsible innovation and ethics mean to you. Identify at least three questions you would ask before supporting or participating in a technology project.
- » Identify at least three transferable abilities you practiced through the course and the evidence you can preserve to demonstrate them.
- » Summarize your 30-, 60-, and 90-day learning plan, including resources, tasks, work samples, feedback, review dates, and an alternative if a resource is unavailable.



- » State the boundary of your current knowledge. Explain which questions require more study or qualified professional guidance.
- » Conclude with a realistic statement of how you intend to continue learning and participating responsibly. Do not promise an outcome that you cannot control.

Your capstone should show critical thinking, self-directed learning, clear writing, ethical judgment, and practical planning. You are not being asked to purchase an asset, create an account, open a wallet, join a community, reveal confidential information, or predict a financial result.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, the capstone title, and the date completed.

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

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Final Capstone — [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 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, employer confidential information, another person's private information, or facility-sensitive information.

UNDERSTANDING WEB3

SECTION 6 AND CUMULATIVE COURSE REVIEW

A Prison Professors Self-Directed Course

Estimated time: 100–140 minutes

Educational and Safety Boundary:

This review provides general education about Web3 applications, careers, ethics, continuing education, and related risks. It does not provide individualized financial, investment, legal, tax, employment, or career advice. No activity requires internet access, an account, a wallet, a digital asset, a purchase, or a transaction. Review Purpose

You have completed Lessons 19 and 20 and reached the final review in Understanding Web3. This review connects real-world applications, conventional alternatives, transferable abilities, evidence, uncertainty, ethics, and continuing education. It also helps you gather the ideas you will need for the final Profile capstone.

I encourage you to begin with the Section 6 questions and scenario. Then complete the cumulative review by explaining the course in your own language. The purpose is to strengthen understanding and judgment. It is not a high-stakes examination.

THE REVIEW COVERS:

- » Evaluating a use case through the problem, proposed solution, evidence, risks, and alternatives.
- » Comparing blockchain designs with ordinary databases, signed documents, established payment systems, trusted intermediaries, and improved procedures.
- » Recognizing transferable abilities and building honest evidence of preparation.
- » Separating established capabilities, active development, forecasts, commitments, promotion, and unanswered questions.
- » Applying responsible innovation, ethics, safety, accountability, and access to a proposed project.
- » Connecting all six sections of the course in preparation for the final capstone.

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 Parts 1 and 2 before reading the scenario in Part 3.
- » Use the printed lessons when you need to check a definition or reconsider an answer. You do not need the internet.
- » Complete Part 4 in your own language. Those notes can become an outline for your final Profile capstone.
- » Do not include passwords, private keys, seed phrases, authentication codes, account numbers, real wallet addresses, or other sensitive information.

ANSWER-KEY REMINDER

This learner-facing review does not include answers. Correct responses, brief rationales, and sample responses will appear in the consolidated appendix.

Attempt every question before consulting the appendix. Compare your reasoning, correct errors on separate paper, and preserve your original work when circumstances permit.

PART 1: KNOWLEDGE QUESTIONS

MULTIPLE CHOICE

1. Which question should come first when evaluating a proposed blockchain use?
 - a. Which token will the project distribute?
 - b. What defined problem needs to be solved, and who experiences it?
 - c. Which network has attracted the most attention?
 - d. How quickly can the project promise a result?
2. Which statement best describes a digital credential?
 - a. A digital claim from an identified issuer that still requires evaluation of the issuer, claim, status, and purpose
 - b. A public record that every employer must accept
 - c. A guarantee that the original information was correct
 - d. A digital asset that must have a market price
3. Which example best demonstrates a transferable ability?
 - a. Repeating a project's promotional description
 - b. Claiming expert status after completing one course



- c. Writing a clear comparison of evidence, risks, and alternatives that another person can review
 - d. Purchasing a digital asset to prove interest in technology
- 4. Which statement is a forecast rather than an established capability?
 - a. A public blockchain records transactions under its network rules.
 - b. A smart contract performs defined functions when called.
 - c. Every employer will use blockchain credentials within two years.
 - d. A public explorer displays selected on-chain records.
- 5. Which action best demonstrates responsible innovation?
 - a. Selecting a blockchain before defining the problem
 - b. Examining purpose, evidence, affected people, safeguards, access, governance, and alternatives
 - c. Removing risk disclosures so participants remain enthusiastic
 - d. Assuming technical capability resolves every ethical question
- 6. Which item is the strongest evidence that a learner is preparing responsibly?
 - a. A statement that the learner is passionate about technology
 - b. A copied promotional description
 - c. A dated collection of original work showing analysis, feedback, revision, and completion
 - d. A promise that future success is certain
- 7. Which statement accurately describes the independent PP token community case?
 - a. Prison Professors created and controls the token.
 - b. The public ledger proves every person's identity, purpose, and future decision.
 - c. An independent community used Web3 tools to support the mission, while public records and future commitments must be described separately.
 - d. The case guarantees that every documented personal story will attract financial support.

TRUE OR FALSE

- » If a blockchain preserves a record against later alteration, the network also guarantees that the original information was accurate.



- » A person can continue developing Web3 knowledge through reading, writing, comparison, correspondence, and case analysis without purchasing an asset or opening an account.

SHORT EXPLANATION

- » A training program claims that its six-week course guarantees a Web3 job and that its token will increase ten times in price. In five to seven sentences, classify the claims, identify evidence that is missing, and explain one safer way to continue learning.

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. Use case
- » B. Digital credential
- » C. Supply chain
- » D. Compliance
- » E. Transferable skill
- » F. Portfolio
- » G. Responsible innovation
- » H. Ethics
- » I. Uncertainty
- » J. Continuing education
- » K. Action plan
- » L. Evidence of preparation

DEFINITIONS

1. A written sequence that identifies an objective, tasks, resources, dates, evidence of completion, and a point for review or adjustment.
2. An organized collection of work that demonstrates knowledge, abilities, progress, and completed projects.
3. A specific problem, task, or process that a technology or service is proposed to address.

4. Principles and reasoning used to evaluate right conduct, duties, harms, fairness, honesty, and responsibility.
5. Intentional learning that continues after a course through study, practice, feedback, reflection, and updated evidence.
6. A claim represented in digital form and issued by an identified source about a person, organization, object, or achievement.
7. The connected people, organizations, processes, goods, and information involved in producing and delivering a product or service.
8. Dated, reviewable work that shows knowledge, skill, effort, reliability, and improvement.
9. The process of understanding and following applicable laws, regulations, contracts, policies, standards, and organizational requirements.
10. An ability that can be useful across different jobs, industries, projects, or stages of a career.
11. A condition in which available knowledge is incomplete, changing, or insufficient for a guaranteed conclusion.
12. The development, use, or evaluation of technology with attention to purpose, evidence, people affected, safety, fairness, privacy, accountability, access, and long-term consequences.

PART 3: APPLIED SCENARIO — THE BRIDGEFORWARD SKILLS RECORD

This scenario is fictional. BridgeForward, SkillCredit, BridgeDollar, and BridgeGov do not represent verified products, partnerships, credentials, or assets. No learner should create an account, open a wallet, purchase an asset, or conduct a transaction to complete this exercise.

A nonprofit called BridgeForward offers education to incarcerated and formerly incarcerated learners. Course records currently remain in separate offices. Participants sometimes wait several weeks for verification, and employers do not always know whom to contact.

A vendor proposes a public-blockchain system. Each participant would receive a wallet and a permanent public identifier. Course completions would be issued as digital credentials. A smart contract would award fictional SkillCredit tokens after each verified completion. The vendor says the system is tamper-proof, fully decentralized, and guaranteed to create employer trust.

The design also includes a fictional stablecoin called BridgeDollar. Donors could place BridgeDollar into a smart contract that lends some of the tokens through a



decentralized-finance protocol. The vendor expects the yield to pay education stipends. The proposal does not explain the stablecoin's reserves, redemption process, borrower standards, collateral, liquidation rules, oracle, withdrawal limits, or legal and accounting review.

BridgeGov tokens would provide voting power over upgrades and the community treasury. Two vendor-controlled addresses hold 61 percent of the voting power. A three-person committee can pause the contracts and approve upgrades. The proposal does not identify the committee members, disclose conflicts, or explain how learners can challenge an incorrect credential.

The project website cites a limited pilot involving 30 participants. It describes that pilot as proof that every major employer will adopt the system within two years. Enrollment requires an immediate token purchase. A countdown message tells readers that waiting will eliminate their opportunity.

A staff member proposes a simpler alternative: keep the records in an accountable non-profit database, issue digitally signed certificates, and provide a telephone and limited online verification service. The alternative would allow corrections, revocation, and account recovery, but it would rely on one organization and its continued operation.

SCENARIO QUESTIONS

1. Define the underlying problem without assuming that either proposal is the solution. Identify the people, current process, failure, and desired result.
2. Describe the blockchain design as connected layers. Include the network, identifiers, wallets, keys, credentials, tokens, smart contracts, stablecoin, oracle, lending system, governance, treasury, administrators, and user interface.
3. Identify at least ten risks or unanswered questions. Include privacy, accuracy, correction, recovery, custody, scams, stablecoin structure, lending, liquidity, smart-contract code, oracle data, voting concentration, administrative control, access, and legal uncertainty.
4. Classify the claims tamper-proof, fully decentralized, guaranteed employer trust, and universal adoption. State what the pilot establishes and what it cannot establish.
5. Compare the blockchain proposal with the database, signed-certificate, and verification-service alternative. Explain which conditions could favor each design and which responsibilities remain under either approach.
6. Recommend rejection, redesign, further research, a limited pilot, the conventional alternative, or a carefully explained combination. Support your conclusion with evidence, safeguards, an accountability process, and one uncertainty that would require later review.

PART 4: CUMULATIVE COURSE REVIEW

Use this part to prepare for the final Profile capstone, What I Learned About Web3 and How I Am Preparing for the Future. Write notes in your own language. You may use short paragraphs or an outline at this stage. Your final capstone should become one coherent 800–1,200-word essay.

1. BUILD A COURSE MAP.

- » Write one or two sentences explaining the principal focus of each of the six sections.
- » Show how a network, digital asset, wallet, smart contract, application, governance process, and human decision can connect.

2. EXPLAIN CENTRAL CONCEPTS.

- » Define blockchain and Web3 in your own language.
- » Explain coins, tokens, stablecoins, wallets, private keys, custody, smart contracts, decentralized applications, decentralized finance, and governance.
- » Choose at least one analogy and state where the analogy stops being accurate.

3. IDENTIFY RECURRING RISKS AND RESPONSIBLE RESPONSES.

- » Select at least four risks or limitations from the course.
- » For each one, explain a responsible response. Consider scams, credentials, privacy, volatility, liquidity, custody, irreversibility, code, oracles, concentrated power, and legal uncertainty.

4. SEPARATE FACTS FROM FUTURE POSSIBILITIES.

- » Explain the difference among an established capability, active development or pilot, forecast, promotion, commitment, and unanswered question.
- » Give one example of at least three categories and identify evidence that could change a conclusion.

5. ANALYZE THE INDEPENDENT PP TOKEN COMMUNITY CASE.

- » Separate the independent community, public blockchain record, transaction-charge rule, public treasury address, my perspective, my reserve commitment, future plans, and unresolved questions.
- » Explain why the case can illustrate community support without recommending an asset or promising that another person's work will produce the same response.



6. DOCUMENT TRANSFERABLE ABILITIES.

- » Identify at least three abilities you practiced, such as research, writing, communication, source evaluation, digital safety, project coordination, customer support, compliance awareness, or critical analysis.
- » Name a dated work sample that could demonstrate each ability.

7. APPLY RESPONSIBLE INNOVATION AND ETHICS.

- » Write at least three questions you would ask before supporting or participating in a technology project.
- » Address purpose, affected people, evidence, safety, privacy, fairness, access, governance, accountability, and alternatives.

8. PREPARE YOUR CONTINUING-LEARNING PLAN.

- » Summarize your 30-, 60-, and 90-day objective, resources, tasks, work samples, feedback, review dates, and alternative if one resource is unavailable.
- » State the boundary of your current knowledge and identify one question that requires more study or qualified guidance.

9. DRAFT YOUR CONCLUSION.

- » Write a realistic statement describing how you intend to continue learning and participating responsibly.
- » Focus on conduct and preparation you can control. Do not promise employment, income, support, adoption, release, or another result controlled by someone else.

COMPLETION CHECK

Before consulting the appendix or drafting your capstone, ask yourself whether you can:

- » Explain the course's major systems and show how technical and human layers interact.
- » Compare blockchain with a simpler alternative without assuming that one design is always stronger.
- » Separate a present capability from a pilot, forecast, commitment, promotion, and open question.
- » Identify security, privacy, financial, legal, operational, access, and governance risks.

- » Explain how ethical conduct and responsible innovation shape technical decisions.
- » Identify transferable abilities and dated evidence that another person can review.
- » Create a realistic continuing-learning plan that fits your current resources and permissions.

If one statement remains difficult, return to the relevant lesson and write a brief explanation in your own words. Then revise your notes. That process demonstrates self-directed learning.

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 6 and Cumulative Course Review, and the date you completed the work.

- » Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Section 6 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, employer confidential information, another person's private information, or facility-sensitive information.

UNDERSTANDING WEB3

CONSOLIDATED APPENDIX: SAMPLE RESPONSES AND ANSWER KEY

A Prison Professors Self-Directed Course

This appendix contains representative responses and answer keys for all 20 lessons and six section reviews. It is designed for learners who may study independently, without internet access or an instructor.

HOW TO USE THIS APPENDIX

Complete your own exercise, knowledge check, Profile assignment, or section review before consulting the corresponding response. Date your work. Then compare your reasoning with the sample.

Objective questions include a correct answer and brief rationale. Open-ended activities include a representative response written in my first-person voice. Those samples are not the only acceptable responses. Your work should use your own reasoning, experience, goals, and language.

When your answer differs, determine whether you misunderstood a concept, used different but accurate wording, or reached another supportable conclusion. Revise on separate paper and preserve your earlier response when circumstances permit. That record can show how your thinking develops.

SAFETY AND SUBMISSION REMINDER

- » Never include a real password, private key, seed phrase, authentication code, account number, wallet address, transaction identifier, or other sensitive credential.
- » No exercise requires an account, wallet, asset, purchase, transfer, vote, application connection, or transaction.
- » Subject to facility rules, responses may be sent by institutional email to Playbook@PrisonProfessors.org.
- » Postal responses may be sent to Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
- » A learner may also send a response to an approved family member or supporter who can enter it in the learner's Profile at PrisonProfessors.org.

CONTENTS BY SECTION

Section 1 — Understanding the Internet and Web3

- » Lesson 1: Becoming Your Own Prison Professor
- » Lesson 2: How the Internet Changed: From the Early Web to Web2
- » Lesson 3: What Is Web3?
- » Lesson 4: Centralization, Decentralization, and Tradeoffs
- » Section 1 Review: Understanding the Internet and Web3

Section 2 — Blockchain Foundations

- » Lesson 5: What Is a Blockchain?
- » Lesson 6: Blocks, Transactions, and Hashes
- » Lesson 7: Nodes, Networks, and Consensus
- » Lesson 8: Comparing Blockchain Networks and Understanding Layers
- » Section 2 Review: Blockchain Foundations

Section 3 — Digital Assets and Tokenization

- » Lesson 9: Cryptocurrencies, Coins, and Tokens
- » Lesson 10: Stablecoins: Uses, Structures, and Risks
- » Lesson 11: Tokenization and Non-Fungible Tokens
- » Section 3 Review: Digital Assets and Tokenization

Section 4 — Wallets, Transactions, and Security

- » Lesson 12: Wallets, Addresses, Keys, and Seed Phrases
- » Lesson 13: Custody and Self-Custody
- » Lesson 14: How a Blockchain Transaction Works
- » Lesson 15: Scams, Security, Privacy, and Irreversible Errors
- » Section 4 Review: Wallets, Transactions, and Security

Section 5 — Smart Contracts, DeFi, and Governance

- » Lesson 16: Smart Contracts and Decentralized Applications
- » Lesson 17: Decentralized Finance
- » Lesson 18: Decentralized Organizations and Governance
- » Section 5 Review: Smart Contracts, DeFi, and Governance

Section 6 — Applications, Skills, and Responsible Preparation

- » Lesson 19: Real-World Applications, Limitations, and Career Skills
- » Lesson 20: Preparing Responsibly for the Future of Web3
- » Section 6 and Cumulative Course Review

SECTION 1 — UNDERSTANDING THE INTERNET AND WEB3

This section reviews self-directed learning, changes in the web, a careful definition of Web3, and the tradeoffs among centralized, decentralized, and mixed systems.

LESSON 1: BECOMING YOUR OWN PRISON PROFESSOR

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

I would begin by writing that I want to understand an emerging part of the digital economy and strengthen my ability to evaluate unfamiliar claims. The two abilities I would emphasize are clear writing and critical thinking.

I would follow a regular cycle: read, define, question, apply, write, and review. If difficult vocabulary or interruption slowed me down, I would return to the definition, write my own example, and resume when conditions allowed. My judgment rules would be to check sources and compare benefits with risks and alternatives. My privacy rules would be never to record a real credential and never to disclose sensitive information because someone created urgency.

Across the 20 lessons, I intend to demonstrate that I can direct my learning, explain what I understand, identify uncertainty, accept correction, and follow through. I would date the commitment and review it after every five lessons.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. C — Set a goal, use available resources, check understanding, and adjust the plan.

Rationale: Those actions show active responsibility for learning and progress.

2. B — The course provides general technology education.

Rationale: It does not provide individualized financial, legal, or tax advice and does not require financial participation.

3. A — A dated journal entry that explains, evaluates, and applies an idea.

Rationale: Original, dated work gives another person evidence of reasoning and follow-through.

4. False.

Rationale: A course and Profile can document preparation, but they cannot guarantee a decision controlled by another person or institution.



SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

I intend to summarize each lesson in my own language before moving forward. That habit tests my understanding and reveals the questions I still need to ask.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

I chose to study Web3 because I believe preparation should begin before an opportunity appears. During 26 years in federal prison, I could not predict how technology or the economy would change. I could decide how I would use each day. Reading, writing, asking questions, and documenting my progress helped me prepare for a future I could not see.

Through this course, I want to understand blockchains, digital assets, wallets, smart contracts, and online communities. I also want to understand their limitations and risks. My objective is not to repeat promotional claims or pretend that I know more than I do. I want to strengthen my ability to explain technical information in plain language and evaluate evidence before reaching a conclusion.

I will work through the lessons in sequence because each lesson builds upon the previous lesson. My routine will include defining vocabulary, completing the offline exercise, answering the knowledge check, and writing a coherent Profile entry. When I encounter a difficult concept, I will return to the source, create my own example, and revise my explanation.

I want my Profile entries to show a pattern of self-directed learning. A dated body of work can show that I set goals, follow through, accept feedback, and correct errors. One important boundary is that these lessons provide education rather than individualized advice. That boundary reminds me to separate learning from a financial decision.

I cannot control which opportunities will open. I can control whether I continue learning, writing, revising, and preparing.

LESSON 2: HOW THE INTERNET CHANGED: FROM THE EARLY WEB TO WEB2

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

I would place items 1, 3, and 5 under an early-web pattern because they primarily describe information published for a visitor to read. I would place items 2, 4, 6, 8, and 12 under a Web2 pattern because they involve accounts, user contributions, interaction, or a platform coordinating participants.

Items 7, 9, 10, and 11 could fit both. A news article or personal page may be a fixed publication, while comments, accounts, personalization, or collaborative editing



create a Web2 pattern. Messaging and search existed in earlier forms but later became deeply connected with accounts, platforms, and user data. The deciding question is not the date alone. I would ask what participants can create, how they interact, and who controls the service.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — The web is one major service operating through the broader internet.

Rationale: The internet is the connected network infrastructure; the web uses that infrastructure.

2. C — Create an account, upload a video, and respond to comments.

Rationale: Accounts, user-created content, and interaction are common Web2 patterns.

3. C — One organization has primary authority over accounts, rules, and systems.

Rationale: Centralization concerns control, even when the service uses many computers.

4. False.

Rationale: Web2 developed over time and did not begin through one universal upgrade.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A centralized learning platform can make information easy to find and can connect teachers with many learners. The tradeoff is that the operator can change access, collect data, remove content, or alter rules, so participants depend on that organization.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Internet services changed communication by allowing people to publish, respond, organize communities, and exchange information across distance. The early web often felt like a collection of pages to read. Web2 added accounts, platforms, user-created content, and ongoing interaction.

User contributions can create substantial value. A learner may post a question, a worker may share experience, and a customer may review a product. Other people benefit from that information, while the platform organizes and stores it. The platform may also receive data, attention, revenue, and control over the relationship.

A centralized service can offer convenience, consistent rules, recovery, moderation, and one accountable operator. The tradeoff is dependence. The operator may suspend an account, change a policy, collect information, or decide which content



remains visible. That does not make every centralized service harmful. It gives me questions to ask before I rely on one.

I would not treat early web and Web2 as rigid categories or exact dates. Technologies and patterns overlap. A site may publish fixed information in one area and support accounts or comments in another.

This history encourages me to strengthen source evaluation and privacy awareness. I want to ask who created the information, which incentives shape it, what data the service collects, and which alternatives remain available. As I move into Web3, my question is: when a service promises greater ownership or control, which technical and human rules actually support that claim?

LESSON 3: WHAT IS WEB3?

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

I would classify claims 1, 2, 6, and 10 as facts or testable capabilities because a reviewer could inspect a blockchain record, code behavior, protocol rules, or the legal boundary between token control and copyright. Claims 3 is an opinion. Claims 4 and 11 are forecasts or aspirations. Claims 5 and 9 are promotional statements.

Claims 7 and 12 use absolute language that turns an unverified conclusion into promotion. Claim 8 is a stated plan; I would classify the plan as a present fact only if the provider documented it, while actual interoperability remains unproven.

My evaluation questions would include: Which record or code supports the claim? Who controls each layer? Which compatible implementations exist? What risk, exception, or dependency has been omitted?

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A broad set of developing technologies and ideas.

Rationale: Web3 is an evolving umbrella term involving blockchains, digital assets, programmable rules, and decentralized designs.

2. A — A public blockchain records token transfers under its protocol.

Rationale: That is an observable capability rather than a forecast or guarantee.

3. C — Interoperability depends on compatible rules, standards, and implementations.

Rationale: A label alone does not make different systems work together.

4. False.



Rationale: A service can use a blockchain while retaining centralized interfaces, administrators, data sources, or governance.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

The statement promises complete control without identifying the system, rules, keys, interfaces, administrators, or limits. I would ask which parts the user controls, who can change the code or account access, and which evidence shows the promised control in practice.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

I define Web3 as a broad and developing group of technologies and ideas that use blockchains, digital assets, smart contracts, wallets, and decentralized designs to create new forms of online interaction. It is not one finished product and does not automatically replace Web2.

Two ideas appear useful to me. A shared ledger may help several organizations inspect the same history without giving one organization sole control. A portable digital credential may help a person present a verified achievement across compatible services. Each use still depends on accurate source information, privacy, governance, and working standards.

One common claim is that Web3 gives every user complete control. I classify that statement as an aspiration or promotional claim, depending on the context. I would ask who controls the website, code, keys, upgrades, data, and governance. I would also look for documentation, a working example, security review, and a process for correcting errors.

A centralized service may remain appropriate when one accountable organization can maintain a private database, provide recovery, correct records, and respond to complaints. A blockchain could add cost or privacy risk without improving the result.

My approach is curiosity with disciplined evaluation. I do not have to accept or reject a system because it uses the Web3 label. I can identify the present capability, the future goal, the control points, and the unresolved questions. The next question I want to examine is how convenience changes when authority is distributed and participants accept more direct responsibility.

LESSON 4: CENTRALIZATION, DECENTRALIZATION, AND TRADEOFFS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

For the bank ledger, I would record one bank as the official controller, bank procedures as the verification and correction process, strong convenience and recovery, dependence on the bank, and limited direct responsibility for ledger maintenance.

For the shared community record, authority is divided among five organizations and three approvals verify updates. Corrections depend on the written agreement. The design reduces dependence on one organization but adds coordination, governance, and shared-security duties.

For the public blockchain, the protocol and network participants verify updates. Confirmed history can be difficult to alter, but authorized corrections may be difficult and public data can reduce privacy. Participants carry greater responsibility for credentials and transaction review.

I would favor an accountable private system for sensitive medical records, a transparent shared ledger for limited public donation records, and a conventional database for a small inventory unless several independent parties truly need shared control.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — Distribution describes where computers work; decentralization describes how authority is divided.

Rationale: A system can use many computers and remain centrally governed.

2. A — An intermediary coordinates, verifies, processes, or settles activity.

Rationale: An intermediary can provide useful functions and also create dependence.

3. C — Central recovery can offer convenience while direct control increases responsibility.

Rationale: That comparison acknowledges benefits and costs on both sides.

4. False.

Rationale: Decentralizing one component does not guarantee that the full service is decentralized, fair, or safe.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

An organization-managed account can provide recovery, support, and one point of responsibility, but the user depends on the operator's rules and continued service.



Direct control can reduce that dependence while making the user responsible for security, backup, verification, and irreversible errors.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Centralization concentrates primary authority in one organization or governing center. Decentralization divides selected authority, operation, or control among several participants. Neither label describes every feature of a system.

A bank account is a centralized service that can offer useful convenience. The bank maintains the official record, provides recovery procedures, and responds to disputes. The tradeoff is dependence on the bank's security, policies, access decisions, and continued operation.

A shared record among several community organizations could benefit from divided control when no single organization should have sole authority. A governance agreement could require multiple approvals and preserve matching copies. The participants would accept responsibility for coordination, data quality, access control, corrections, and dispute resolution.

Decentralization does not guarantee fairness or safety. Voting power may concentrate, participants may not understand their duties, and responsibility may become unclear. A centralized system can also fail or abuse authority. I need to compare the actual design rather than the label.

Before choosing, I would ask: Who can change the record or rules, and who corrects an error? I would also ask: Which design fits the privacy, recovery, efficiency, accountability, and resilience needs of the people affected?

The lesson strengthens my ability to compare alternatives. A responsible recommendation can favor a centralized, decentralized, or mixed design when the reasons are clear and the remaining responsibilities are acknowledged.

SECTION 1 REVIEW: UNDERSTANDING THE INTERNET AND WEB3

PART 1: KNOWLEDGE QUESTIONS

1. B.

Rationale: Self-directed learning involves goals, resources, monitoring, and adjustment.

2. A.

Rationale: The course provides general education and does not promise an individual result.



3. B.

Rationale: The web operates through the broader internet.

4. B.

Rationale: Accounts, video uploads, and comments reflect a participatory Web2 pattern.

5. C.

Rationale: A centralized service concentrates primary authority in one organization.

6. C.

Rationale: Web3 is a broad and developing group of technologies and ideas.

7. B.

Rationale: The statement describes an observable blockchain capability.

8. False.

Rationale: Web2 developed gradually rather than through one official date.

9. True.

Rationale: Technical work may be distributed while governance remains centralized.

QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

Decentralization divides selected authority or operation, but it can still concentrate wealth, voting power, technical influence, or access. It may create slower decisions or unclear responsibility. I would ask which problem the design is trying to solve, who controls the rules, who can correct an error, and who remains accountable after a failure.

PART 2: VOCABULARY MATCHING

- » 1. L — Tradeoff
- » 2. F — Platform
- » 3. E — Web2
- » 4. J — Centralization
- » 5. C — Internet
- » 6. A — Self-directed learning
- » 7. H — Protocol
- » 8. D — Early web
- » 9. K — Decentralization
- » 10. B — Critical thinking

- » 11. I — Permissionless
- » 12. G — Web3

PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. Design A concentrates authority in one nonprofit. Design B divides authority among the four organizations through synchronized copies and multiple verification.
2. Under Design A, the operating nonprofit should investigate and correct an inaccurate listing. Under Design B, the governance agreement should identify who receives a report, investigates the source, approves a correction, and communicates the result.
3. Design A may allow faster routine correction because one organization can act. The tradeoff is greater dependence on its staffing, security, policies, and continued operation.
4. Design B may remain available after one organization fails, but I would need evidence that the copies are synchronized, systems can operate independently, credentials are protected, and no shared provider creates a hidden point of failure.
5. Design B needs correction and dispute rules, membership and replacement rules, access permissions, data standards, emergency procedures, and a way to resolve a tie.
6. I would recommend a combination: one accountable service for routine administration, shared oversight for important policy changes, and regular backups held by participating organizations. The group would still need written governance, security, correction, and continuity procedures. A different recommendation could be reasonable if the evidence and responsibilities support it.

SECTION 2 — BLOCKCHAIN FOUNDATIONS

This section reviews ledgers, blocks, transactions, hashes, nodes, consensus, network comparisons, and the relationships among base networks, scaling systems, and applications.



LESSON 5: WHAT IS A BLOCKCHAIN?

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

The three ledgers begin at 20 and show balances of 17, 22, and 18 after the authorized transactions. Ledger C changes the second transaction and ends at 19. Comparing copies reveals the disagreement, while the original authorized list and shared rule provide the basis for correction.

Matching copies can show agreement, but they cannot make false source information true. The paper simulation represents shared copies, grouped records, sequence, verification, and disagreement. It leaves out computers, digital signatures, cryptographic links, formal consensus, incentives, security, and network governance.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A shared digital ledger that groups records into linked blocks.

Rationale: A blockchain maintains an ordered record under network rules.

2. A — Linking helps preserve order and reveal changes to earlier history.

Rationale: Later blocks refer to earlier records, making inconsistent alteration detectable.

3. C — Several organizations need a shared record without one party holding sole control.

Rationale: That coordination need can justify evaluating a blockchain against simpler alternatives.

4. False.

Rationale: Agreement shows what the network accepted, not whether the original source was honest or accurate.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A blockchain can help several participants maintain and inspect one shared history without relying on one recordkeeper. Its limitations include privacy, cost, governance, inaccurate source data, and difficult correction, so decision-makers should compare it with an ordinary database.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

I describe a blockchain as a shared digital ledger maintained by a network. Proposed records are verified under shared rules, grouped into blocks, and linked in order so that later changes to earlier history become easier to detect.

A shared record could help several education organizations verify course completions without giving one office sole control. The system might improve consistency and resilience. It would still need accurate source information, privacy protections, permission rules, correction procedures, governance, and accountability.

The strongest lesson for me is that agreement is not the same as truth. If an authorized person enters false information, a blockchain may preserve the false entry. A durable record can make correction more difficult. I would ask who supplies the data, how identity is verified, who can correct an error, what information becomes public, and whether a simpler database would perform the task more responsibly.

The comparison strengthens my critical thinking because it separates capability from promotion. I can explain a possible benefit without assuming that every problem requires a blockchain. My practical takeaway is to define the problem first, examine evidence and risks, and compare alternatives before recommending a system.

LESSON 6: BLOCKS, TRANSACTIONS, AND HASHES

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

The original toy hashes are 09, 16, and 23. Changing Block 1 from five books to six changes its toy hash to 10. Block 2 no longer points to the matching earlier result; after recalculation it becomes 17, and Block 3 becomes 24.

The mismatch reveals that earlier data changed. The change affects later references because each later calculation includes the prior result. The toy hash does not prove whether five or six books were actually received. A person trying to preserve the altered chain would have to recalculate every later reference. Real systems add secure hash functions, digital signatures, validation, consensus, and distributed software.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. A — Proposal, checking, block selection, network agreement, and recording.

Rationale: A transaction is proposed and evaluated before accepted recording.

2. B — A fixed-length result representing input data and helping detect change.

Rationale: A hash changes when its input changes; it is not the same as reversible encryption.

3. A — A later block includes a reference derived from earlier data.

Rationale: Changing earlier data changes the derived reference and breaks later links.

4. False.

Rationale: A matching hash shows consistency with recorded data, not outside truth or lawful authorization.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

Tamper-evident means an unexpected change leaves evidence that can be detected. Tamper-resistant means the design makes an accepted alteration difficult. Neither term means that change is impossible under every technical, governance, or network condition.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A blockchain transaction is a proposed update. A node checks basic rules, a block producer may include it in a proposed block, and the network's consensus process determines whether the block becomes part of the accepted history.

A hash is a fixed-length result derived from input data. If the input changes, the result changes. A later block can contain a hash-based reference to an earlier block, so changing earlier data causes the later reference to stop matching.

That design supports tamper evidence and resistance, but it does not create an absolute guarantee. An attacker, administrator, or network majority may have different capabilities under different systems. Careful wording avoids the claim that a record is impossible to change.

A matching hash can show that the compared data is unchanged from the recorded version. It cannot prove that the original statement was true, that the signer acted lawfully, or that the human purpose was satisfied. This distinction strengthens my communication. I want to describe what evidence supports without extending the conclusion beyond that evidence.

LESSON 7: NODES, NETWORKS, AND CONSENSUS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Rule A relies on one coordinator, so dishonest or mistaken control concentrates in that person. Rule B uses computational effort and later accumulated work; power may concentrate among participants with greater equipment or energy. Rule C uses committed value, selection, approvals, and penalties; power may concentrate among large holders, delegates, or service providers.

None of the rules proves how many books arrived. They only determine which proposed record the participants accept. The recordkeepers still need an authorized delivery document, independent count, inspection, or another outside source.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A computer running network software.

Rationale: Nodes may store, relay, check, or propose data depending on their role.

2. A — Agreement on an accepted blockchain history.

Rationale: Consensus manages disagreement among distributed participants under network rules.

3. B — Proof of work uses computational effort; proof of stake uses committed value and validator rules.

Rationale: Each method relies on different resources and incentives.

4. False.

Rationale: Many nodes receive, relay, store, or verify data without producing blocks.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

Consensus shows that network participants accepted a record under their rules. It does not independently inspect a delivery, identity, contract, or statement from the outside world. Accuracy still depends on authorized sources and evidence.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A node is a computer running blockchain software. Some nodes store, relay, or check information. A miner or validator is a participant with a defined role in proposing or approving blocks, so the terms are not interchangeable.

A consensus mechanism helps distributed participants choose an accepted history. Proof of work uses computational work and accumulated effort. Proof of stake uses committed value, validator selection, voting, rewards, and possible penalties. Proof of work can create security through costly competition but may concentrate power around equipment and energy. Proof of stake can reduce that energy demand but may concentrate influence among large holders or service providers.

Neither process proves that outside information is true. A network can agree that an authorized transaction was recorded while the source document was false or the signer lacked lawful authority.

I would trust a shared system only after examining its rules, participation, concentration, software, history, governance, and response to failure. The lesson strengthens my ability to separate technical agreement from human truth and to ask which evidence supports each conclusion.

LESSON 8: COMPARING BLOCKCHAIN NETWORKS AND UNDERSTANDING LAYERS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Bitcoin, Ethereum, and BNB Smart Chain are Layer 1 base networks. opBNB is described as a Layer 2 system connected with BNB Smart Chain. The fictional credential system belongs primarily at the application layer.

For each row, I would compare purpose, dependencies, possible benefits, risks, and missing evidence. Price is a poor technical criterion because it does not establish security, performance, governance, suitability, or access. For a credential system, I would emphasize privacy, issuer authority, correction, recovery, and dependable verification. I would write unknown—needs verification wherever the lesson does not supply enough evidence.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. A — The network is the shared system; the native asset is one component.

Rationale: A network includes ledger, consensus, nodes, and rules beyond the asset.

2. B — A base blockchain with its own ledger and consensus rules.

Rationale: That is the course definition of Layer 1.

3. C — Ask what it processes, posts to the base network, and depends on.

Rationale: A Layer 2 must be evaluated through its relationship and new dependencies.

4. False.

Rationale: Layer 3 has no single universal definition across all projects.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A higher layer number is a category, not a quality score. Faster advertised speed can omit security, finality, congestion, operator, or bridge dependencies. A more expensive native asset also does not prove that the network fits a particular purpose.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Networks should be compared through consistent criteria rather than price or promotion. I would examine purpose, consensus, participation, performance, finality, programmability, dependencies, governance, and access.

A blockchain network is the shared technical system. Its native asset is built into the protocol and may support fees or security. A Layer 1 maintains its own ledger and consensus history. A Layer 2 processes or organizes activity in a defined relationship with a Layer 1. The application layer provides a service that interacts with



one or more networks. Layer 3 must be defined whenever it is used because projects use the label differently.

Bitcoin and BNB Smart Chain are both Layer 1 networks, but their purposes, consensus designs, programmability, participation, and governance differ. opBNB depends on BNB Smart Chain and introduces its own operators, software, and connection risks.

A layered system may increase capacity or reduce some fees. It can also add bridges, sequencers, interfaces, and failure points. If a promoter says one system is best because it is faster or popular, I would ask for measurements, conditions, security assumptions, and alternatives. The comparison process helps me organize evidence and communicate a reasoned conclusion without relying on slogans.

SECTION 2 REVIEW: BLOCKCHAIN FOUNDATIONS

PART 1: KNOWLEDGE QUESTIONS

1. B.

Rationale: A blockchain is a shared ledger of linked blocks maintained under network rules.

2. A.

Rationale: A transaction moves from proposal and checking toward network agreement and recording.

3. B.

Rationale: A hash is a fixed-length result used to represent data and detect change.

4. B.

Rationale: A node can store, relay, or check data without producing blocks.

5. A.

Rationale: Consensus helps distributed participants agree on accepted history.

6. A.

Rationale: Proof of work and proof of stake use different resources and both have tradeoffs.

7. C.

Rationale: A Layer 2 must be evaluated through its base network relationship and added dependencies.

8. True.

Rationale: Consensus can accept a record without proving every outside claim.

9. False.

Rationale: Layer 3 does not have one universal definition.



QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

A matching hash shows that data matches the version used to create the recorded result. Consensus shows that participants accepted a record under their network rules. Neither process independently verifies the truth, identity, or lawful authority behind outside information. A signed source document, authorized issuer record, physical inspection, or correction review could provide additional evidence.

PART 2: VOCABULARY MATCHING

- » 1. C — Transaction
- » 2. K — Layer 1
- » 3. B — Ledger
- » 4. I — Proof of stake
- » 5. A — Blockchain
- » 6. D — Hash
- » 7. F — Node
- » 8. J — Native asset
- » 9. E — Tamper-evident
- » 10. H — Proof of work
- » 11. G — Consensus mechanism
- » 12. L — Layer 2

PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. The completion submission is the transaction. Accepted transactions are grouped into a block. The hash reference links the block to earlier history. Each organization runs a node, while selected validators propose or approve blocks.
2. The hash link can reveal an inconsistent change to earlier recorded data. It cannot prove that the learner completed a course or that the issuer entered accurate information.
3. Consensus can establish the accepted shared history under the rules. Identity, completion, issuer authority, consent, and correction still require outside evidence and human review.
4. Committed value, validator selection, voting, and penalties suggest proof of stake. I would request the distribution of stake, selection method, penalty rules, software, governance, and evidence of independent participation.



5. The provider must identify the Layer 1, data posted there, security relationship, operator control, failure process, and recovery path.
6. A blockchain may reduce reliance on one recordkeeper and support shared inspection, while adding technical, privacy, governance, and correction burdens. One trusted database may offer clear accountability and recovery while creating dependence on one organization. I would recommend a limited requirements review and pilot using fictional data before selecting either design.

SECTION 3 — DIGITAL ASSETS AND TOKENIZATION

This section reviews coins, tokens, liquidity, stablecoin structures, tokenization, non-fungible tokens, metadata, authenticity, rights, and the evidence needed to evaluate digital-asset claims.

LESSON 9: CRYPTOCURRENCIES, COINS, AND TOKENS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

BaseUnit is a native asset because it is built into the base protocol. CoursePass and CommunityVote are tokens created on existing networks. StudyPoints is a conventional database entry. FutureSkill is described as a planned token, but its real function and market conditions remain unknown.

For each item I would identify the supported function, controlling network or organization, restrictions, and missing evidence. A function does not prove value or liquidity. The word utility does not establish use, demand, safety, issuer reliability, market depth, or legal classification.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A digital asset native to its own blockchain.

Rationale: The course uses coin for a native blockchain asset.

2. C — Verify the function, control, restrictions, and dependencies.

Rationale: A label and one displayed price do not establish practical utility.

3. B — Exchange without excessive delay or a large price change.

Rationale: Liquidity concerns market depth and execution conditions.

4. False.

Rationale: Technical function does not guarantee value, compliance, liquidity, or protection from fraud.



SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

Labels can be inconsistent and can hide dependencies. I would identify the network, code, function, rights, control, evidence, liquidity, risks, and simpler alternatives before accepting a broader claim.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Cryptocurrency is a broad label. In this course, a coin or native asset is built into its own blockchain protocol. A token is created through code on an existing blockchain. Industry usage varies, so technical structure is more reliable than the label alone.

Digital assets may pay network fees, support security, provide access, represent a vote, or track a defined claim. Those functions are different from an investment promise. The word utility does not prove that people need the token, that a market is liquid, or that the project complies with applicable requirements.

Before accepting a claim, I would ask: Which network and contract identify the asset? What function works now? Who controls the code, interface, supply, and upgrades? Which rights are defined? What evidence supports use and liquidity? Which risks and alternatives remain?

The independent PP token case helps separate evidence from accountability. A public blockchain can show selected token transfers, contract activity, and a public treasury balance. It cannot prove every participant's identity, why every transfer occurred, how private credentials are protected, or how future resources will be used.

A conventional database or membership account may be simpler when one accountable organization provides access and correction. The evaluation process strengthens my judgment because I replace a label with questions another person can review.

LESSON 10: STABLECOINS: USES, STRUCTURES, AND RISKS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

ReserveDollar provides the clearest stated redemption path, but eligibility, timing, fees, reserve quality, and custody still require verification. CollateralDollar depends most directly on volatile crypto collateral, oracle prices, and liquidation. BalanceDollar depends most heavily on continuing market confidence and program rules without a separate reserve.

For each description I would document the reference value, support mechanism, redemption route, control, evidence, and stress risks. I would request independent reserve information, custody details, collateral levels, oracle procedures, code



review, governance, liquidity, and legal terms. A shared stablecoin label does not make different mechanisms equally safe.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A token designed to track a stated reference value.

Rationale: The design objective is not a guarantee.

2. C — Ask what supports it, who holds support, who can redeem, and what evidence exists.

Rationale: Reserve quality and redemption rights shape risk.

3. A — Redemption follows system rules; a market sale depends on a buyer and liquidity.

Rationale: The two exit routes can differ in access, price, delay, and fees.

4. False.

Rationale: Past price stability does not remove reserve, redemption, technology, liquidity, or legal risk.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

Two one-dollar targets can rely on different reserves, collateral, code, issuers, redemption rights, markets, and governance. Those dependencies can produce different loss and depeg pathways even when both tokens trade near the same reference today.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A stablecoin is a token designed to track a reference value. Stable describes an objective; it does not mean risk-free or insured.

A reserve-backed design depends on assets held by an issuer or custodian and on defined redemption rules. A crypto-collateralized design depends on pledged digital assets, oracle prices, collateral ratios, and liquidation. An algorithmic design relies more heavily on program rules, incentives, market demand, and continuing confidence.

Direct redemption means returning the token through an issuer or protocol process under stated conditions. A secondary-market sale depends on another buyer, available liquidity, price impact, and market access.

In the fictional ReserveDollar case, I would identify the one-dollar reference and claimed reserve. I would still request independent evidence about reserve assets, custody, eligible redeemers, timing, fees, and stress procedures. A loss of confidence, impaired reserve, blocked redemption, or thin market could cause a depeg.

I would not treat a stablecoin as an insured bank deposit without evidence of the account structure and applicable protection. This analysis strengthens my research and communication because it requires me to describe the mechanism, evidence, and uncertainty rather than trust the name.

LESSON 11: TOKENIZATION AND NON-FUNGIBLE TOKENS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

The token record can support that token ID 1842 exists under a contract, an address received it on a recorded date, and the recorded transfer history shows no later transfer. The contract's connection to LearningBridge, course completion, learner identity, file availability, employer recognition, correction authority, and issuer authority require outside evidence.

I would request an official issuer statement, signature or verified contract record, privacy-preserving identity process, metadata and storage policy, revocation procedure, recovery method, and recognition criteria. The token may add value when several parties need portable verification and the issuer, identity, storage, and correction layers are reliable.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — Use a digital token to represent an item, record, right, claim, or access.

Rationale: Tokenization represents something through a token; it does not prove the represented claim.

2. C — A distinguishable token commonly identified by a contract and token ID.

Rationale: Uniqueness does not guarantee value or rights.

3. C — Ask who issued it, what the record proves, and what outside evidence supports it.

Rationale: Authenticity depends on issuer authority and reliable connections.

4. False.

Rationale: Token control does not automatically transfer copyright, title, identity, or every related right.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A blockchain token is one record layer. The referenced file, physical item, credential, legal right, issuer authority, and recognition may exist outside the blockchain. Each layer requires separate evidence and governing rules.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Tokenization uses a digital token to represent an item, record, right, claim, or access. An NFT is tracked as a distinguishable token, usually through its network, smart contract, and token ID.

The token is not automatically the file, service, credential, or legal right it references. Metadata may describe the item or provide a storage location. That file can change or disappear. Contract control also does not prove that an issuer had authority to make the claim.

In the LearningBridge scenario, the blockchain may show that token 1842 exists and that a receiving address obtained it on a recorded date. Course completion, learner identity, issuer authority, employer recognition, storage continuity, correction, and revocation still require outside evidence.

Token control does not automatically transfer copyright because copyright depends on law and agreement, not only address control. A tokenized credential may support portable verification and tamper evidence. Its risks include privacy exposure, incorrect data, lost access, unavailable files, false issuers, and unclear recognition.

An ordinary credential database or signed certificate can offer simpler correction, recovery, and accountability. Tokenization may add value when several independent verifiers need a portable record and the complete system protects identity, storage, rights, and correction. I would choose based on the problem rather than novelty.

SECTION 3 REVIEW: DIGITAL ASSETS AND TOKENIZATION

PART 1: KNOWLEDGE QUESTIONS

1. A.

Rationale: A token is created and recorded through code on an existing blockchain.

2. B.

Rationale: BNB is native to BNB Smart Chain; PP and WBNB are tokens on the network.

3. B.

Rationale: Liquidity concerns exchanging without excessive delay or price movement.

4. C.

Rationale: Reserve assets, custody, evidence, and redemption rules must be examined.

5. A.



Rationale: Redemption follows system rules; a market sale depends on buyers and liquidity.

6. C.

Rationale: The token, metadata, storage, referenced item, and rights may exist in separate layers.

7. B.

Rationale: Issuer, record, evidence, and recognition determine credential reliability.

8. False.

Rationale: Utility does not guarantee value, liquidity, compliance, or safety.

9. True.

Rationale: Failures in support or confidence can cause a depeg.

QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

A blockchain can record a token but does not create a stability mechanism by itself. A stablecoin claim requires evidence about reserves or collateral, redemption, markets, code, and governance. A tokenized certificate also requires issuer authority, reliable identity connection, metadata storage, correction, recognition, and governing rights. I would request independent reserve evidence and a verified issuer and credential process before accepting the combined claim.

PART 2: VOCABULARY MATCHING

- » 1. K — Metadata
- » 2. D — Liquidity
- » 3. L — Authenticity
- » 4. A — Native asset
- » 5. E — Stablecoin
- » 6. G — Redemption
- » 7. B — Token
- » 8. I — Tokenization
- » 9. C — Utility
- » 10. F — Reserve
- » 11. J — Non-fungible token
- » 12. H — Depeg



PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. PathCoin is the native asset. StudyDollar is a fungible token described as a stablecoin. CompletionPass 742 is an NFT.
2. StudyDollar targets the United States dollar and claims cash and short-term investments as support. The issuer and custodian are not identified clearly, and direct redemption is unexplained. I would request independent reserve reports, custody records, redemption eligibility, timing, fees, and legal terms.
3. Redemption follows an issuer or protocol process. A market sale requires a buyer and sufficient liquidity. Thin markets or lost confidence can push the market price away from the target.
4. The blockchain may show the contract, token ID, receiving address, and transfer history. Learner identity, completion, issuer authority, file availability, correction, recognition, and legal rights require outside evidence.
5. Address control proves control of the token under the contract, not copy-right, personal identity, course completion, or employer acceptance. Meta-data and authenticity links must be evaluated separately.
6. The tokenized design may support portable verification but adds privacy, storage, custody, and governance burdens. Ordinary payments and a signed database credential may offer simpler recovery and accountability but depend on one operator. I would test requirements, privacy, correction, and verifier acceptance before selecting a design.

SECTION 4 — WALLETS, TRANSACTIONS, AND SECURITY

This section reviews wallets, addresses, keys, seed phrases, custody, transaction stages, public evidence, privacy, scams, and irreversible errors.

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

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

A public receiving address and transaction identifier may be public in the right context. A private key, seed phrase, password, and authentication code must remain secret. Network information and every unexplained signature request belong under Verify before acting. A balance screenshot may expose a public address and transaction patterns, so sharing it requires a privacy decision.

A public address identifies a destination but does not grant signing authority. A private key authorizes actions. A password may protect an application, while a seed



phrase can recreate keys and accounts. If anyone requests a secret or unexplained signature, I would stop, refuse, verify independently, and seek trusted help.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A tool for viewing records, managing credentials, and authorizing actions.

Rationale: Assets remain recorded on the blockchain; the wallet manages interaction.

2. C — A private key.

Rationale: A private key can authorize transactions and must remain secret.

3. A — The corresponding key authorized specific data that was not altered after signing.

Rationale: A signature does not prove wisdom, ownership, or personal identity.

4. False.

Rationale: A seed phrase and application password have different purposes and are not interchangeable.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A public address can let observers locate balances and transactions under network rules. It does not reveal the private key or give an observer signing authority. The same public history can still expose patterns and reduce privacy.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A blockchain wallet helps a person view network records, prepare instructions, and use signing credentials. The digital assets remain recorded on the blockchain rather than sitting physically inside the wallet.

A public address is a shareable destination. A private key is a secret that creates signatures and authorizes actions. A signature can show that the relevant key approved specific data without exposing the key itself. It does not prove the signer's full identity or the wisdom of the action.

A seed phrase may recreate many keys and accounts, which makes it more powerful than an ordinary application password. Both require protection, but losing or disclosing a seed phrase can affect every account derived from it.

The public Prison Professors treasury address illustrates transparency and confidentiality. Observers can inspect selected balances and transfers while the signing credentials remain private. The public history still creates privacy and targeting risks.



My rules are direct: I will never share a seed phrase, private key, password, or authentication code. I will not sign data I do not understand. I will verify the network, purpose, identity, and instructions through an independent source. Careful credential management demonstrates responsibility because trust depends on protecting authority as well as documenting public evidence.

LESSON 13: CUSTODY AND SELF-CUSTODY

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Jordan can continue learning without an account; current facility rules make action unavailable. Renee may value third-party recovery, but she should examine provider control, access limits, and counterparty risk. Luis may value direct control but needs secure backups and an incapacity plan. The nonprofit needs written authority, multiple-person review, recovery, continuity, and transparent reporting rather than one director holding sole signing power.

Each profile produces a different balance of control, convenience, recovery, access, counterparty risk, and personal responsibility. The next question should identify missing facts without prescribing a product or transaction.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A provider controls keys or the signing process.

Rationale: The user depends on the provider to carry out authorized requests.

2. C — Cold storage concerns connection; self-custody concerns control.

Rationale: The concepts answer different questions.

3. A — Another party may fail, misuse authority, block access, or break an agreement.

Rationale: That dependency is counterparty risk.

4. False.

Rationale: Key control does not prove legal ownership, wise judgment, or a recovery plan.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

The phrase warns that a custodian's control can limit a user's access. It does not resolve legal rights, provider safeguards, recovery, personal capability, institutional rules, or whether direct control creates a greater practical risk.



PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Custody concerns who controls the credentials or process that authorizes an action. In a custodial arrangement, a provider controls the keys or signing system. In self-custody, the person or organization controls them directly.

Third-party custody may offer convenience, customer support, and recovery, while creating counterparty risk and dependence on the provider's rules. Self-custody may reduce that dependence, while increasing responsibility for device security, backups, recovery, transaction review, and continuity.

Cold storage describes how credentials are kept relative to online use. Self-custody describes who controls them. A provider can use cold storage, and an individual can use hot self-custody.

The public Prison Professors treasury address can show selected on-chain balances. It does not show the private signing arrangement, approval rules, backup, recovery, or legal authority. Those facts require written policies and accountable reporting.

A person who lacks secure backup conditions may reasonably value provider recovery. A technically prepared organization may value direct control when it also has multiple-person authorization and continuity procedures. Institutional rules may prevent action today, but they do not prevent learning.

The responsible analysis asks where control sits, what recovery requires, which parties must be trusted, and who can act after illness or failure. That process supports judgment and credibility without prescribing one arrangement for everyone.

LESSON 14: HOW A BLOCKCHAIN TRANSACTION WORKS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

The best sequence is F, B, C, D, G, A, E, H: assemble, review, sign, broadcast, validate, include and execute, reach confirmations or finality, and inspect the receipt.

Preparation can introduce a wrong address, network, asset, amount, action, or fee. A valid signature cannot prevent deception or poor judgment. Broadcast proves submission, not inclusion or success. A rejected transaction never enters the accepted block; an included failure may execute unsuccessfully and still use a fee. A technically successful transfer to the wrong destination can fail its human purpose. Reconciliation should compare the on-chain record with internal authority, amount, purpose, and accounting.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — The relevant key authorized the specific transaction data.



Rationale: A signature proves key authorization, not wisdom or destination identity.

2. A — Submission to a node without a guarantee of inclusion or success.

Rationale: Broadcast is an intermediate stage.

3. C — A valid transaction sends an asset to the wrong address.

Rationale: The network can process instructions correctly while the human purpose fails.

4. True.

Rationale: An included smart-contract failure may still consume network resources and a fee.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A transaction hash identifies a recorded transaction, and success reports execution under network rules. Neither establishes the signer's intent, lawful authority, correct destination, off-chain agreement, accounting treatment, or ethical purpose. Those conclusions require additional records and review.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A blockchain transaction is a signed instruction asking a network to update its shared state. A wallet or service assembles the fields, a reviewer checks the network and details, the authorized key signs, a node broadcasts, the network validates, a block producer includes and executes, and later confirmations lead toward finality.

The signature shows authorization by the relevant key for the specific data. It does not prove identity, ownership, wisdom, consent free from deception, or a correct destination. A transaction hash locates the record. A confirmation shows inclusion under network-specific rules. Finality describes when reversal becomes sufficiently unlikely or restricted under that network.

A rejected transaction is not accepted. An included failure may consume a fee while the requested contract action fails. A successful mistake executes exactly as instructed but sends value or authority to the wrong place.

The public Prison Professors treasury record can show selected transfers and balances. It does not establish custody, accounting, ownership, purpose, or mission results by itself.

Transaction discipline begins before signing and continues afterward. I would verify details independently, use a second review for organizational actions, wait



for the appropriate network result, and reconcile the on-chain record with internal authorization. That patience and verification support responsibility and trust.

LESSON 15: SCAMS, SECURITY, PRIVACY, AND IRREVERSIBLE ERRORS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Message A uses urgency and requests a password and code. Message B promises an impossible match and demands secrecy. Message C builds emotional trust, guarantees success, and requests another payment. Message D impersonates support and asks for a seed phrase. Message E copies a mission, creates urgency, supplies an unverified destination, and promises doubling.

For every message I would Stop, avoid the supplied link or number, Verify through previously trusted information, and Seek Help from an authorized person. I would disclose no password, private key, seed phrase, code, or financial information. My rule is to create distance between pressure and authorization.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A request for a seed phrase or private key.

Rationale: Legitimate support should never need the secret that grants control.

2. C — Use previously verified contact information.

Rationale: The sender must not control the verification channel.

3. C — Selected on-chain activity recorded under network rules.

Rationale: A public record does not prove motive, identity, or a promise.

4. False.

Rationale: A central help desk ordinarily cannot require reversal of a finalized blockchain transaction.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

Stop creates time and prevents an impulsive reply or signature. Verify uses a separate channel and trusted record that the sender did not provide. Seek Help adds another person's judgment before any secret or value is exposed.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A scam can persuade an intelligent person because it targets emotion, trust, routine, and time pressure rather than intelligence alone. Urgency narrows attention. Secre-



cy prevents outside review. Fear, hope, affection, and authority can push a person toward action before verification.

Three warning signs that cause me to pause are a request for a secret, a guaranteed return or recovery, and pressure to use a supplied destination immediately. I would apply Stop, Verify, Seek Help. I would not reply or use the link. I would contact the organization through information I already trust and ask an authorized person to review the request.

A seed phrase, private key, password, and authentication code must remain confidential because each can grant access or support unauthorized action. Public blockchain records can help verify selected activity, but repeated address history may reduce privacy and help an impersonator create a convincing story.

Irreversibility increases the cost of a rushed error. The fictional Prison Professors message uses a real mission label to support an unauthorized request. A legitimate mission does not make an unfamiliar account or destination authentic.

My rules are to slow down, refuse secrecy, verify identity and destination independently, protect every credential, and seek a second review before authorization. I would rather miss a supposed opportunity than surrender control to pressure.

SECTION 4 REVIEW: WALLETS, TRANSACTIONS, AND SECURITY

PART 1: KNOWLEDGE QUESTIONS

1. B.

Rationale: A wallet helps view records, prepare transactions, and use signing credentials.

2. A.

Rationale: A public address is designed for receiving and locating activity.

3. B.

Rationale: A seed phrase is a powerful recovery secret.

4. C.

Rationale: Custodial and self-custodial arrangements distribute control and risk differently.

5. A.

Rationale: A valid signature shows authorization by the relevant credential.

6. B.

Rationale: Correct network execution can still produce an unintended human result.



7. C.

Rationale: Stop, verify independently, and seek help.

8. False.

Rationale: Private-key control does not automatically prove legal identity or ownership.

9. True.

Rationale: Public history can reduce privacy, and final transfers may be difficult to reverse.

QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

A public address can show selected on-chain activity but does not authenticate a message sender. Cold storage describes how credentials are kept, not who controls them or which approvals apply. A familiar logo can be copied. I would stop, verify through previously trusted contact information, compare the destination and network with authorized records, obtain a second review, and disclose no secret.

PART 2: VOCABULARY MATCHING

- » 1. H — Broadcast
- » 2. F — Counterparty risk
- » 3. J — Phishing
- » 4. A — Wallet
- » 5. C — Private key
- » 6. I — Confirmation
- » 7. E — Self-custody
- » 8. D — Seed phrase
- » 9. L — Irreversible transaction
- » 10. B — Public address
- » 11. G — Transaction fee
- » 12. K — Social engineering

PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. Warning signs include urgency, copied identity, an unfamiliar channel, a new destination, a supplied link, a seed-phrase request, unexplained contract approval, no second reviewer, one-person control, and an advance-fee recovery offer.

2. A public address, public balance, network name, and transaction history may be public. Private keys, seed phrases, passwords, codes, and internal recovery information must remain secret. Public information does not authenticate the sender.
3. The wallet prepares and signs; custody identifies who controls authorization; self-custody means the organization controls its credentials; cold storage concerns connection. The team still needs written facts about control, backups, approval, and recovery.
4. The sequence is preparation, review, signature, broadcast, validation, confirmation, and finality. The team can correct ordinary errors before signing and broadcast.
5. Stop all action. Verify through previously trusted contact information and authorized internal records. Seek help from the responsible officer, board reviewer, security professional, or institution.
6. Future requests should require written authority, two-person review, destination and network verification, limited approvals, custody and recovery procedures, privacy review, suspicious-message escalation, and an absolute rule against sharing secrets.

SECTION 5 — SMART CONTRACTS, DEFI, AND GOVERNANCE

This section reviews programmed rules, decentralized applications, oracles, audits, decentralized finance, liquidity, lending, governance, delegation, treasuries, and human accountability.

LESSON 16: SMART CONTRACTS AND DECENTRALIZED APPLICATIONS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Case A produces APPROVE ONE CREDIT because the source is authorized, completion is reported, and no previous credit exists. Case B produces REJECT because the source is unauthorized. Case C produces REJECT because the input says not completed, even though the human fact differs. Case D produces REJECT because the identifier already has a credit, revealing an identity-design failure.

People or outside systems supplied participant codes, reports, authorization status, and prior records. The rules omitted correction, appeal, identity conflict, and second review. I would add a rule that disputed or conflicting inputs pause automatic approval and route the case to an authorized human review before the state becomes final.



KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — Code deployed on a blockchain that performs defined functions when called.

Rationale: A smart contract executes programmed rules; it does not independently judge fairness.

2. C — An application using smart contracts plus interfaces and supporting components.

Rationale: A dapp can include both decentralized and centralized layers.

3. A — To obtain selected information from outside the blockchain.

Rationale: An oracle supplies data but cannot guarantee its accuracy.

4. False.

Rationale: An audit covers a defined scope and time and cannot guarantee future safety.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

The PP token contract can automate a programmed transaction charge and direct the defined portion toward an address. Code does not decide whether the mission is worthy, whether communications are accurate, how resources should be governed, or whether future use fulfills a commitment. People remain accountable for those judgments.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A smart contract is code deployed at a blockchain address that performs defined functions when called. A decentralized application combines one or more contracts with an interface, network, wallets, data services, and human controls.

Code can apply a consistent fee rule or reject an input that does not meet a condition. Correct execution does not guarantee a fair or useful human result. If the input is wrong or the rule omitted an appeal, the code can produce an incorrect outcome exactly as written.

In the completion-credit example, the input includes participant code, report, source authorization, and prior state. The rule approves or rejects, the state records earlier credit, and the output is a decision. A duplicate identifier or incorrect report reveals missing identity and correction conditions.

An oracle supplies outside information such as a price or completion report. Incorrect, delayed, or manipulated data can trigger the wrong output. An audit can identify weaknesses within its scope, but cannot guarantee complete safety or cover later upgrades.



I would keep identity disputes, appeals, mission decisions, and final accountability subject to human review. Written routines can support my self-directed learning, just as code supports consistency, but neither replaces reflection, feedback, and revision.

LESSON 17: DECENTRALIZED FINANCE

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

RiverBridge's possible yield comes from borrower interest and RIVER incentives. Borrower payments depend on continued borrowing and repayment. A falling RIVER price can reduce the value of incentives. Collateral value, oracle data, liquidation, stablecoin support, pool liquidity, smart-contract code, governance, and administrator powers create additional dependencies.

A displayed balance does not prove immediate withdrawal liquidity. Possible depositor losses include code failure, bad debt, illiquidity, depeg, incentive decline, oracle error, and governance changes. Borrower losses include liquidation, collateral decline, fees, oracle error, and contract failure.

I would rewrite the advertisement this way: The protocol describes a variable return funded by borrower interest and token incentives. Returns, principal, and withdrawal access can change because of market, liquidity, collateral, oracle, code, stablecoin, and governance risks.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — Blockchain services using smart contracts for financial-like functions.

Rationale: DeFi is a broad category, not a guarantee of safety or decentralization.

2. B — Tokens held for exchanges under a pricing formula.

Rationale: A liquidity pool supplies the assets used by an automated market maker.

3. A — Collateral falls below the required threshold.

Rationale: Liquidation can protect the protocol while creating loss for the borrower.

4. False.

Rationale: Higher possible return generally adds dependencies, uncertainty, or loss pathways.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A DeFi protocol can use smart contracts to calculate exchanges, manage collateral, or apply lending rules. It still depends on developers, administrators, interfaces, available



liquidity, market prices, oracles, governance, stablecoin issuers, and participant security. Automation changes how the function operates; it does not remove people or risk.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

Decentralized finance describes blockchain-based services that use smart contracts for exchange, lending, borrowing, liquidity, or related functions. The label does not prove that every layer is decentralized.

A decentralized exchange can use a liquidity pool and formula to calculate a token exchange. The independent PP/WBNB pair illustrates two tokens held in a BNB Smart Chain pool. The pool, contract, interface, network, community, and Prison Professors organization remain separate components.

In lending, a borrower pledges collateral. If its reported value falls below the required threshold, the protocol may liquidate. Yield may come from borrower interest, trading fees, incentive tokens, a treasury, or another strategy. Every source has conditions and can weaken.

Liquidity risk can prevent an expected exchange or withdrawal. Oracle risk can trigger an incorrect price, liquidation, or accounting result. Administrators and governance may repair problems while also concentrating authority.

A promise of greater return should produce more questions because I need to identify who pays, what supports the payment, which asset carries the return, how principal can be lost, and whether an exit is available. I can document those questions before reaching a conclusion. That process demonstrates disciplined learning without requiring financial participation.

LESSON 18: DECENTRALIZED ORGANIZATIONS AND GOVERNANCE

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

The member distribution totals 100 units. One-person-one-vote follows the number of people supporting each position; token-weighted voting follows the assigned units. The same preferences can produce different results because influence is distributed differently.

Members C through J hold 40 units and do not reach a 50-unit quorum. Members A and B hold 60 and can reach quorum despite representing only two people. Equal ten-unit allocations change the result toward the member count.

Delegation can improve informed participation but can concentrate influence and create conflicts. The proposal needs scope, budget, recipient, milestones, conflicts,

security review, authorization, and reporting. Emergency authority should be narrow, explained publicly, time-limited, and reviewed after use.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A community using blockchain rules and collective procedures.

Rationale: A DAO coordinates selected decisions or resources; people remain responsible.

2. B — Assign voting power to a representative.

Rationale: Delegation can improve participation and concentrate influence.

3. B — Larger holders or delegates may control active voting power.

Rationale: Token distribution and turnout shape influence.

4. False.

Rationale: A successful vote proves authorization under rules, not fairness, lawfulness, security, or success.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A token can calculate voting power, a public treasury can show selected transfers, and a communication channel can host discussion. Responsible DAO governance also requires defined membership, proposals, participation, conflict disclosure, security, execution rules, reporting, accountability, and evidence that votes have meaningful effect.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

A DAO is a community that uses blockchain-based rules and collective procedures to coordinate selected decisions or resources. A governance token may calculate voting power without proving equal influence or legal rights.

A responsible process begins with a clear proposal, discussion, disclosed conflicts, technical and financial review, understandable voting terms, quorum, voting, a useful delay, execution, and public reporting. Membership count and voting power differ. Ten people may participate while two large holders control the outcome.

In the Second Chance Learning Treasury, token-weighted voting can let Members A and B reach quorum with 60 units while eight smaller members cannot. Equal voting units produce a different result. Delegation may let a prepared representative review complex proposals, but it can concentrate authority and create conflicts or weak oversight.



Quorum can prevent decisions with very low participation. A timelock creates time for review. Narrow emergency authority can protect the system when its scope, explanation, duration, and later review are defined.

Public treasury transfers show on-chain movement, not whether off-chain work was completed. The independent PP token community should not be called a DAO without evidence of formal governance.

A responsible, transparent, and fair process provides understandable information, meaningful participation, disclosed conflicts, protected execution, and follow-up reporting. In my own work, I can document decisions, seek feedback, disclose incentives, and accept responsibility for results.

SECTION 5 REVIEW: SMART CONTRACTS, DEFI, AND GOVERNANCE

PART 1: KNOWLEDGE QUESTIONS

1. B.

Rationale: A smart contract is deployed code that stores data and performs defined functions.

2. C.

Rationale: A dapp can include interfaces, contracts, networks, wallets, outside data, and human controls.

3. B.

Rationale: Incorrect or manipulated oracle data can trigger a wrong result.

4. A.

Rationale: A liquidity pool supplies tokens used for exchanges or other functions.

5. A.

Rationale: Collateral below the threshold may become eligible for liquidation.

6. C.

Rationale: A reviewer should trace the return source, conditions, and loss pathways.

7. B.

Rationale: Delegation assigns voting power and can concentrate influence.

8. False.

Rationale: An earlier audit cannot guarantee every component or future upgrade.

9. True.

Rationale: A rule-following vote can still reflect concentrated power.



QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

Audited may identify a prior technical review, but I would ask which version and components it covered. Community controlled does not establish broad participation or distributed power. An 18 percent yield is a stated rate, not proof of a sustainable return or protection from loss. I would examine current code, audit scope, administrator powers, oracle data, liquidity, collateral, return sources, voting distribution, conflicts, and legal uncertainty.

PART 2: VOCABULARY MATCHING

- » 1. O — Treasury
- » 2. C — Oracle
- » 3. H — Liquidity pool
- » 4. K — Yield
- » 5. L — Decentralized autonomous organization
- » 6. A — Smart contract
- » 7. D — Audit
- » 8. I — Collateral
- » 9. G — Decentralized exchange
- » 10. N — Delegation
- » 11. E — Vulnerability
- » 12. F — Decentralized finance
- » 13. M — Governance token
- » 14. B — Decentralized application
- » 15. J — Liquidation

PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. OpenPath includes an interface, contracts, network, wallet interactions, oracle, administrative committee, and governance. A false oracle input can trigger contract liquidation and financial loss.
2. The oracle price is the input, the collateral threshold is the rule, the loan and collateral are stored state, and liquidation is the output. Incorrect data or code can produce an incorrect sale.
3. Yield comes from borrower interest and PathGov incentives. Loss pathways include borrower default, collateral decline, oracle failure, illiquidity, reward-token decline, contract defects, governance changes, and stablecoin failure.



4. Two addresses hold 64 percent of voting power, participation is low, and a paid delegate may have conflicts. A quorum and many addresses do not remove concentrated influence.
5. The audit is old and limited. Community control is weakened by concentrated votes and emergency powers. Safer data and higher yield lack testing, simulations, independent review, and clear evidence.
6. I would separate the four changes, require conflict disclosure, obtain current technical and oracle review, analyze collateral and liquidity, document treasury authority, extend the waiting period, narrow emergency powers, and publish execution and performance reports.

SECTION 6 — APPLICATIONS, SKILLS, AND RESPONSIBLE PREPARATION

This section reviews real-world applications, limitations, transferable skills, evidence of preparation, responsible innovation, and a practical plan for continued learning.

LESSON 19: REAL-WORLD APPLICATIONS, LIMITATIONS, AND CAREER SKILLS

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

Problem: PathwayPass wants to help employers verify training credentials that come from several providers. The current problem is fragmented records and slow verification.

Proposed solution: Approved training providers could issue digital credentials that a learner can present. An employer could check whether a credential came from an authorized issuer and whether its status changed.

Evidence I would seek: I would ask for a clearly defined user need, interviews with learners and employers, a working pilot, privacy testing, correction and recovery procedures, cost comparisons, accessibility testing, and evidence that employers will use the system.

Risks and limitations: Incorrect source records could become easier to verify without becoming true. Public or linkable data could expose personal information. A learner could lose access to credentials. Employers might reject the format. Standards could remain incompatible. Administrators could retain extensive control. Cost and complexity could exceed the value.

Alternatives: A conventional database, digitally signed certificate, printed record with a verification number, or secure telephone and web verification may solve the problem with less complexity. My recommendation would depend on the parties that need to share control, the sensitivity of the information, and the results of a limited pilot.



KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — Begin with a defined problem.

Rationale: A technology should be evaluated against a specific human need rather than adopted because its label is popular.

2. A — A digital credential.

Rationale: A digital credential can represent an achievement and allow another party to verify selected information.

3. C — A transferable skill.

Rationale: Research, clear writing, evidence review, and risk analysis can apply across industries and roles.

4. False.

Rationale: A blockchain can preserve a submitted record without proving that the original information was accurate.

SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

A careful Web3 case analysis can show that I know how to define a problem, research unfamiliar information, distinguish evidence from promotion, compare alternatives, identify risks, and explain a recommendation in clear language. That portfolio evidence can support a conversation about my preparation, but it cannot guarantee employment.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

I would evaluate a Web3 proposal by defining the problem, identifying the people affected, mapping each technical and human component, examining evidence, identifying risks, comparing alternatives, and stating what I still do not know.

The process develops transferable abilities. I practice research when I locate reliable information. I practice critical thinking when I separate a capability from a forecast. I practice communication when I explain a complex idea in plain language. I practice project planning when I define steps, responsibilities, and evidence of completion.

One portfolio item I could create is a dated case study of a credential-verification proposal. I would explain the problem, proposed design, control points, privacy concerns, correction process, evidence, alternatives, and recommendation. I would preserve revisions so a reviewer could see how I responded to feedback.

The independent PP token community provides another example. I can document the public blockchain record, distinguish it from Prison Professors as an organization, describe my perspective, and identify open questions about governance, communication, and future use. I would not claim that the case guarantees a similar result for another person.

My next step is to select one real-world problem, complete a one-page evidence map, and write a balanced evaluation. I can use that work to strengthen my Profile and show how I learn, reason, and follow through.

LESSON 20: PREPARING RESPONSIBLY FOR THE FUTURE OF WEB3

OFFLINE EXERCISE — MICHAEL'S SAMPLE APPROACH

During the first 30 days, I will organize my course notes, review vocabulary, correct misunderstandings, and complete any missing Profile entries. I will write a one-page explanation of blockchain, Web3, and responsible evaluation for a reader who has not taken the course.

During days 31 through 60, I will select one practical use case and research it through available books, printed materials, or trusted guidance. I will map the problem, participants, technology, evidence, risks, alternatives, and unresolved questions. I will request feedback when that option exists and revise the analysis.

During days 61 through 90, I will complete a polished portfolio case study, update my biography or release plan to reflect the skills I practiced, and identify the next course, book, or project that can deepen my knowledge. I will review the plan at the end of each 30-day period and record what I completed, what changed, and what I will do next.

The evidence will include dated notes, original explanations, completed exercises, revisions, feedback, a finished case study, and a new learning goal. The plan requires no wallet, asset, account, purchase, or internet connection.

KNOWLEDGE CHECK — ANSWERS AND RATIONALES

1. B — A public blockchain records transactions under its protocol.

Rationale: That is an established capability that can be inspected without predicting universal adoption.

2. C — Check purpose, evidence, people, safeguards, access, governance, and alternatives.

Rationale: Responsible innovation evaluates the entire system and the people affected.

3. C — Dated original work showing feedback and revision.

Rationale: A sustained record provides stronger evidence of preparation than an unsupported claim.

4. False.

Rationale: Repetition or the speaker's reputation does not transform a forecast into a verified fact.



SHORT EXPLANATION — MICHAEL'S SAMPLE RESPONSE

An established capability describes something a system can demonstrably do today, such as record a valid transaction under its rules. A forecast describes what someone believes may happen later, such as widespread employer adoption. I would support the first with current technical evidence and label the second as uncertain.

PROFILE JOURNAL ASSIGNMENT — MICHAEL'S SAMPLE RESPONSE

What I Learned About Web3 and How I Am Preparing for the Future

I chose this course because I believe that preparation begins before an opportunity appears. During 26 years in federal prison, I learned that I could not control every condition around me, but I could control whether I read, wrote, asked questions, and documented my progress. Self-directed learning helped me build knowledge and credibility over time. I approached Web3 with the same discipline. I did not expect one course to make me an expert. I expected it to strengthen my ability to understand an emerging technology, evaluate claims, and communicate what I learned.

A blockchain is a shared ledger maintained under network rules. Transactions contain proposed changes. Nodes receive and check information. Consensus helps the network agree on valid history. Blocks, hashes, and confirmations help organize and protect that history. Those features can reduce dependence on one recordkeeper, but they do not make every source record accurate, every participant honest, or every application useful.

Web3 is a broad and developing group of technologies and ideas that may include blockchains, digital assets, wallets, smart contracts, and decentralized designs. A coin is generally native to a blockchain, while a token is created through rules on an existing network. Stablecoins attempt to maintain a reference value, but their reserve, redemption, market, code, and governance structures create different risks. Non-fungible tokens can represent distinct records, yet token control does not automatically transfer copyright or guarantee the truth of an off-chain claim.

A wallet helps a person view blockchain activity, prepare a transaction, and use signing credentials. A public address can be shared for receiving or locating activity. A private key or seed phrase is secret and must never be disclosed. Custody describes who controls authorization credentials. Self-custody can reduce dependence on an intermediary, while placing more responsibility on the person or organization. A transaction may be technically valid and still go to the wrong destination, use the wrong network, approve an unsafe contract, or produce an unintended result.



A smart contract is code deployed on a blockchain that performs defined functions. A decentralized application combines contracts with an interface, wallets, network services, data sources, and human controls. Decentralized finance uses these tools for functions such as exchange, lending, borrowing, and liquidity. Decentralized governance may use tokens, proposals, delegation, quorum, voting, and a treasury. In each area, people define rules, provide inputs, control upgrades, respond to failures, and accept responsibility.

Four risks stand out. First, scams and social engineering can use urgency, impersonation, or false recovery promises to obtain secrets or authorization. Second, irreversible errors can make recovery difficult after a transaction is signed and confirmed. Third, smart-contract, oracle, liquidity, collateral, and stablecoin failures can create losses even when code executes as designed. Fourth, governance or administrative power can concentrate behind a decentralized label. Privacy, legal uncertainty, incompatible standards, and unequal access add further concerns.

I also learned to separate an established capability from a pilot and a forecast. An established capability can be demonstrated now, such as a network recording a valid transaction. A pilot is a limited test under stated conditions. A forecast describes a possible future, such as widespread adoption or a predicted price. I should date each claim, identify its source, examine the evidence, and state uncertainty openly.

The independent Prison Professors token community gives me a practical case. The public record can show transactions and a visible treasury address. In Lesson 9, we provided a dated snapshot showing more than 943 WBNB and a smaller native BNB balance. That record is observable, while the meaning and future use require additional context. My perspective is that the community formed independently after learning about the Prison Professors mission. Neither Prison Professors, CZ, nor I created, organized, managed, or controlled the token project. The observed result is that transaction charges generated resources directed to a publicly visible address. I stated an intention to reserve those resources for at least one year. That commitment can be compared with the public record over time. A prediction about future value or impact would remain a forecast. An open question is which governance, security, reporting, and distribution procedures should guide any later use.

Responsible innovation begins with a defined human problem. I should identify the people affected, the evidence, the control points, privacy and security safeguards, access barriers, correction and appeal procedures, governance, and realistic alternatives. A blockchain may be useful when independent parties need a shared record and do not want one party to hold sole authority. A conventional database may be



better when one accountable organization can protect private information, correct errors, and operate efficiently.

This course helped me practice transferable skills: research, source evaluation, vocabulary development, comparison, risk analysis, ethical judgment, clear writing, and project planning. I can demonstrate those abilities through dated Profile entries, completed exercises, revisions, feedback, and a balanced case study. That evidence cannot guarantee a job, release decision, partnership, or financial result. It can help another person see how I prepare and how I respond to new information.

My 30-day goal is to organize my notes, review vocabulary, correct errors, and complete missing Profile entries. By 60 days, I will analyze one practical use case and compare it with a conventional alternative. By 90 days, I will revise that work into a portfolio case study, update my Profile, and select my next learning project. I will measure progress through dated writing and completed revisions.

My present knowledge has limits. I understand foundational concepts and evaluation questions, but I am not qualified to provide individualized financial, legal, tax, cybersecurity, or technical advice. When a decision could affect money, rights, privacy, or security, I would seek current guidance from a qualified professional and verify the facts independently.

I finish this course with greater confidence in my ability to learn, not with a claim that I can predict the future. I can continue preparing, documenting my work, accepting correction, and making responsible decisions. That is how I intend to turn time into an asset and build a record that may support future self-advocacy and opportunity.

SECTION 6 AND CUMULATIVE COURSE REVIEW

PART 1: KNOWLEDGE QUESTIONS

1. B.

Rationale: A sound evaluation begins with a clearly defined problem.

2. A.

Rationale: A digital credential can represent and help verify an achievement.

3. C.

Rationale: Transferable skills can be demonstrated across fields and roles.

4. C.

Rationale: A pilot is a limited test under stated conditions.

5. B.

Rationale: Responsible innovation evaluates the entire system and the people affected.

6. C.

Rationale: A dated portfolio with revisions provides evidence of preparation.

7. C.

Rationale: Qualified guidance is appropriate when a decision affects money, rights, privacy, or security.

8. False.

Rationale: A record can preserve false or incomplete source information.

9. True.

Rationale: A practical plan identifies actions, evidence, review points, and adjustments.

QUESTION 10 — MICHAEL'S SAMPLE RESPONSE

The advertisement combines an unsupported employment guarantee with a price forecast. Neither claim is established by a six-week course, a known speaker, or the existence of a token. I would ask for independently verified employment outcomes, employer requirements, the method and assumptions behind the price prediction, complete risk disclosures, costs, conflicts, and legal terms. A safer learning option would use printed lessons, writing exercises, case analysis, and feedback without requiring a token purchase or financial participation.

PART 2: VOCABULARY MATCHING

- » 1. K — Digital credential
- » 2. F — Pilot
- » 3. A — Use case
- » 4. H — Transferable skill
- » 5. J — Portfolio
- » 6. B — Evidence
- » 7. C — Limitation
- » 8. L — Responsible innovation
- » 9. D — Forecast
- » 10. E — Established capability
- » 11. I — Qualified guidance
- » 12. G — Learning plan



PART 3: APPLIED SCENARIO — MICHAEL'S SAMPLE RESPONSE

1. BridgeForward is trying to address fragmented training records and slow employer verification. I would confirm the problem through learners, training providers, employers, and staff before selecting a technology.
2. The design includes a blockchain network, participant identifiers, wallets, keys, digital credentials, tokens, smart contracts, a stablecoin, an oracle, a lending feature, governance, a treasury, administrators, and an interface. Each layer creates a separate dependency and control question.
3. Risks include privacy exposure, inaccurate source records, difficult correction, lost credentials, custody failure, scams, stablecoin failure, DeFi loss, oracle error, concentrated voting power, broad administrator authority, unequal access, and legal uncertainty.
4. “Tamper-proof” is too absolute because credentials, code, governance, keys, and source data can fail or change. “Fully decentralized” requires evidence about every layer. “Guaranteed employer trust” is an unsupported promise. “Universal adoption” is a forecast, not a present capability.
5. I would compare the proposal with a nonprofit database, digitally signed certificates, printed credentials with verification numbers, and telephone or web verification. The comparison should examine cost, privacy, correction, recovery, accessibility, security, employer acceptance, and governance.
6. I would not recommend the full proposal as described. I would complete further research, remove the token, stablecoin, and lending features unless a defined need justifies them, and test the simplest credential-verification approach in a limited conventional pilot. Any later blockchain pilot should use minimal personal data, clear consent, recovery and correction procedures, independent security review, defined administrators, accessible offline alternatives, and published results.

CUMULATIVE REVIEW SAMPLE OUTLINE

Course map: Begin with internet history and Web3, then move through blockchain foundations, digital assets, wallets and security, smart contracts and governance, and finally applications and responsible preparation.

Central concepts: Explain ledgers, blocks, hashes, nodes, consensus, networks, coins, tokens, stablecoins, wallets, custody, transactions, smart contracts, dapps, DeFi, and governance in plain language.



Risks: Include fraud, credential loss, irreversible error, privacy exposure, code failure, oracle error, illiquidity, volatility, concentrated governance, legal uncertainty, and unequal access.

Fact versus forecast: Date claims, identify sources, distinguish established capabilities from pilots and predictions, and state unresolved questions.

Prison Professors case: Separate the independent community project from Prison Professors, connect observable public records with clearly labeled perspective and commitment, and avoid promotion or a financial recommendation.

Transferable skills: Point to dated writing, research, comparison, risk analysis, ethical judgment, revision, and follow-through.

Responsible innovation: Define the problem, identify affected people, examine evidence and safeguards, assign accountability, compare alternatives, and preserve access for people without technology.

Action plan: Set 30-, 60-, and 90-day goals with specific work products and review points.

Conclusion: State what you understand, which limits remain, which qualified guidance may be needed, and how you will continue learning.

DEVELOPMENT SOURCE NOTE

Drafted July 23, 2026, from the approved 20 lessons, approved Section Reviews 1–5, approved Section 6 and Cumulative Course Review, approved Preface, and controlling Course Blueprint Version 1.1. The appendix introduces no new biographical claim. Time-sensitive course examples remain dated as they appear in the approved lessons.

