

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.

