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

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.

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 copyright, personal identity, course completion, or employer acceptance. Metadata 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.