LESSON 11: TOKENIZATION AND NON-FUNGIBLE TOKENS

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

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

OPENING GUIDANCE

A token can carry a confident label: certificate, ticket, membership, artwork, title, or ownership. The label may describe an intended relationship, but it does not prove that the relationship is valid.

I encourage you to separate the digital record from the claim attached to it. Ask who created the token, what the token points to, what rights the issuer promised, what evidence supports the promise, where important information is stored, and whether another person or institution recognizes the result.

That habit is useful far beyond Web3. A document, badge, database entry, or certificate has value because people can verify who issued it, what it means, and whether the issuer had authority. Technology can strengthen part of that process. It cannot make an unsupported claim true.

This lesson will not ask you to create, purchase, transfer, or display a token. It will help you evaluate what a token record can establish and what still depends on off-chain evidence, legal rights, storage, and human judgment.

PURPOSE AND ESSENTIAL QUESTION

Lesson 11 explains how tokens can represent access, records, rights, or unique items while separating the blockchain token from the underlying legal or practical claim.

Essential Question:

» What does a token record actually prove, and what must be verified somewhere else?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- Define tokenization, fungible, and non-fungible token.
- Distinguish a token record from the item, file, service, credential, or legal right it may reference.
- Identify possible uses in credentials, tickets, property records, creative work, and membership.
- Explain how metadata and storage choices affect a tokenized system.
- Evaluate ownership, copyright, authenticity, privacy, fraud, and legal limitations while comparing tokenization with an ordinary database.

KEY TERMS

TOKENIZATION

Definition: The process of using a digital token to represent an item, record, right, claim, or form of access. The token and the thing it represents are related but not automatically identical.

Sample sentence: The organization considered tokenization for course certificates but first examined whether a conventional credential database would meet the same need.

FUNGIBLE

Definition: Interchangeable with another unit of the same type and value.

Sample sentence: One unit of a fungible token is designed to be equivalent to another unit of the same token.

NON-FUNGIBLE TOKEN

Definition: A distinguishable blockchain token identified separately from other tokens, commonly by a smart-contract address and a token identification number. An NFT can reference an item or claim without containing or legally controlling that item or claim.

Sample sentence: The non-fungible token had its own identification number, but the learner still investigated what rights came with it.

METADATA

Definition: Information that describes other data, such as a token's name, description, image location, certificate details, or attributes.

Sample sentence: The metadata listed the course title and completion date and pointed to an external certificate file.

OWNERSHIP

Definition: A relationship of control or legal rights over property, a record, or an asset. Control of a token does not automatically establish ownership of everything the token references.

Sample sentence: The agreement explained whether token ownership included access, a license, or only control of the token itself.

AUTHENTICITY

Definition: The quality of being genuine and connected to the claimed source.

Sample sentence: The verifier checked the issuer's identity and authority before accepting the tokenized certificate as authentic.

MAIN LESSON

TOKENIZATION CREATES A REPRESENTATION

Tokenization connects a digital token with something else. That something might be access to an event, membership in a community, a course credential, a record about a physical item, a creative work, or a financial or legal interest.

The word represent is important. A paper ticket represents permission to enter an event, but the piece of paper does not create the event. A vehicle title represents a legally recognized relationship with a vehicle, but the title is not the vehicle. A course certificate represents an issuer's statement that a person met stated requirements, but the certificate is not the learning itself.

A blockchain token works in a similar way. The blockchain can record that a particular token was created, assigned, or transferred under the rules of a smart contract. Whether the token delivers a valid ticket, credential, license, property right, or membership benefit depends on more than the blockchain entry.

Tokenization can organize a relationship. It cannot supply missing authority, evidence, or legal recognition.

FUNGIBLE AND NON-FUNGIBLE DESCRIBE HOW UNITS ARE TREATED

Fungible units are designed to be interchangeable. If two people exchange equal units of the same fungible token, neither person is supposed to receive a uniquely distinguished unit.

Non-fungible tokens are tracked separately. A common NFT standard assigns each token a distinct identification number within a smart contract. The complete identifier depends on more than the number alone. A careful description includes the blockchain network, the smart-contract address, and the token ID. Two unrelated contracts can both issue a token numbered 100.

Non-fungible does not mean that the associated picture, file, or idea cannot be copied. It means the token record is distinguishable. A unique token can still be meaningless, fraudulent, technically broken, or disconnected from a real benefit.

AN NFT HAS SEVERAL CONNECTED LAYERS

A beginner can understand an NFT by separating five layers:

1. Network and smart contract: The blockchain and code that create and manage the token.
2. Token record: The token ID, current blockchain address, and transfer history recorded under the contract's rules.
3. Metadata: Information describing the token and often pointing to a file or external record.
4. Referenced item or service: The image, ticket, certificate, physical object, membership, or other subject connected to the token.
5. Rights and recognition: The agreement, policy, law, issuer, institution, or community that gives the token practical or legal meaning.

These layers may work together, but they can also separate. The token can continue to exist after an event is canceled. The metadata can point to a file that is later removed. The physical item can be damaged. The issuer can stop honoring a membership benefit. A license can limit how a creative work may be used. A government record can remain the legally controlling record even if a separate token claims to represent the same property.

The strongest analysis follows the complete chain from code to real-world recognition.

WHAT THE BLOCKCHAIN RECORD MAY ESTABLISH

Under the rules of a functioning network and smart contract, a public blockchain record may help a verifier determine:

- Which smart contract created or manages the token.
- Which token ID is being examined.
- Which blockchain address currently controls the token according to the contract.
- When the token was created or transferred on that network.
- Whether the contract permits transfers, approvals, destruction, pausing, or updates.
- Which metadata location or other data the contract currently returns.

Those facts create a shared history that different participants may inspect.

Even these conclusions require care. A blockchain address does not identify a human being by itself. A transfer record shows what the network accepted; it does not automatically show whether the transfer was voluntary, authorized under an outside agreement, or recognized by law.

WHAT THE BLOCKCHAIN RECORD CANNOT PROVE BY ITSELF

A token record does not automatically prove:

- That the person who created the token owned or had authority over the referenced item.
- That an image or file is original rather than copied.
- That the physical item exists, remains in good condition, or matches its description.
- That the holder received copyright, trademark, property title, or another legal right.
- That a ticket issuer will admit the holder to an event.
- That a school, employer, licensing body, court, or government agency recognizes a credential or record.
- That the person presenting the token controls the identity named in the metadata.
- That off-chain information will remain available, accurate, private, or unchanged.

This boundary is central to the lesson. A blockchain can preserve evidence about a token. It cannot independently verify every fact outside the blockchain.

METADATA CAN CONNECT THE TOKEN TO INFORMATION STORED ELSEWHERE

NFT standards commonly allow a token to provide a location for metadata. The metadata may contain a name, description, image link, certificate information, or other attributes. It may be stored directly on a blockchain, on a decentralized storage system, or on an ordinary web server.

Storing a large file directly on a blockchain can be expensive and may create privacy or permanence problems. For that reason, many NFT-associated files are stored somewhere else. The blockchain token then points to the location.

THIS DESIGN CREATES DEPENDENCIES:

- A web server can stop operating or change the file.
- A link can break.
- A decentralized storage reference may remain valid while the content is no longer readily available.
- Metadata may be updateable by an administrator, which can be useful for corrections but can also change what the token appears to represent.
- Permanent public storage may conflict with privacy, correction, or deletion needs.

Examine the phrase stored on the blockchain precisely. Is the entire file on-chain, or only a token ID and link? Is the metadata fixed or changeable? Who controls updates? What happens if the external location disappears?

TOKEN CONTROL, POSSESSION, CONTRACT RIGHTS, AND COPYRIGHT ARE DIFFERENT

The word ownership can hide several separate relationships. Token control concerns the functions a blockchain address may exercise. Possession concerns control of the referenced copy or object. Contract rights come from stated terms, such as event admission or membership access. Copyright includes legal rights related to an original creative work. Owning a copy of a painting does not normally mean owning the copyright in the painting. The same separation applies to an NFT and an associated work.

A March 2024 report from the United States Copyright Office and United States Patent and Trademark Office explained that transferring an NFT transfers the digital token but does not necessarily transfer the associated asset or copyright rights. A separate agreement is ordinarily needed to transfer copyright or other associated rights. That United States report is dated legal context, not advice about a particular token or transaction.

The practical lesson is durable: read the actual terms. Ask whether the token provides access, a personal-use license, commercial rights, a claim against an issuer,

possession of an object, or only control of the token. Do not let the word owner replace that investigation.

AUTHENTICITY DEPENDS ON THE ISSUER AND THE EVIDENCE

A blockchain can make a record difficult to alter without detection, yet still preserve false information. If an unauthorized person creates a token that points to someone else's artwork, the blockchain can accurately record the unauthorized token.

Authenticity therefore begins with the source. Who is the issuer? How can a verifier connect the issuer's real identity with the issuing smart contract or address? Did the issuer have authority over the referenced item? What process did the issuer follow before creating the token? Is there an outside record, signed statement, institutional policy, or recognized registry that supports the claim?

The same reasoning applies to a tokenized certificate. A verifier must know whether the named institution issued it, whether the recipient completed the work, whether the credential remains valid, and whether the token is linked responsibly to the correct person.

CREDENTIALS DO NOT REQUIRE NFTS OR BLOCKCHAINS

Digital credentials can be designed in many ways. The World Wide Web Consortium's Verifiable Credentials standard describes an issuer, a holder, and a verifier. It includes ways to secure claims against tampering without requiring every credential to be an NFT or a public blockchain record.

The goal should guide the technology. A signed digital certificate, controlled database, standards-based verifiable credential, or blockchain token might address parts of a school's need. The best design depends on access, privacy, correction, revocation, cost, interoperability, governance, and trust.

POSSIBLE USES REQUIRE DIFFERENT KINDS OF RECOGNITION

Tokenization may be proposed for several purposes:

- Tickets: A token may identify an admission credential, but the organizer must recognize it and address mistakes or lost access.
- Membership: A token may unlock services, but the organization must define benefits, duration, transfer, and recovery.
- Credentials: A token may reference an achievement, but issuer identity, assessment, privacy, and revocation still matter.
- Creative work: An NFT may reference art, music, or writing, while creator authorization, storage, license terms, and copyright remain separate.

» Physical property or records: A token may track an object or proposed interest, but a registry, contract, institution, or law may control the recognized right.

In the United States, legal treatment depends on facts and circumstances. A January 2026 statement from three divisions of the Securities and Exchange Commission explained that tokenized securities can use different structures and provide different rights. A third-party token may not provide the same rights as the underlying security and may add counterparty risk. The broader lesson applies beyond securities: tokenization does not change the underlying claim by magic.

BNB SMART CHAIN CAN HOST TOKENS, BUT THE NETWORK DOES NOT VALIDATE EVERY CLAIM

BNB Smart Chain is compatible with the Ethereum Virtual Machine and related smart-contract tooling. Developers can therefore deploy token contracts using interfaces similar to widely used Ethereum standards.

This technical compatibility explains how an NFT can exist on BNB Smart Chain. It does not show that a particular NFT is authentic, valuable, authorized, or legally effective. The network can process the smart contract and record transfers while the associated claim remains false, incomplete, or dependent on an outside agreement.

The recurring BNB Chain example reinforces a distinction used throughout this course: a platform can provide technical capability without endorsing every project built on it.

WHEN AN ORDINARY DATABASE MAY WORK BETTER

A blockchain may add value when independent participants need a shared history, public verification is appropriate, and the benefits outweigh cost, privacy, governance, and error risks.

An ordinary database may work better when one organization already has clear authority, records require correction or deletion, personal information should remain private, users need reliable recovery, activity is high-volume and inexpensive, or outside institutions recognize only the organization's official records.

For an event organizer that controls issuance, admission, refunds, and customer service, a centralized ticket database may provide simpler correction and recovery. A token may add portability or programmable rules while also introducing wallet access, fees, scams, privacy concerns, and irreversible errors. Compare complete systems and ask which approach solves the problem with acceptable cost, access, accountability, and risk.

A DISCIPLINED TOKENIZATION EVALUATION

Before accepting a tokenization claim, ask:

1. Subject: What item, service, record, right, or claim does the token supposedly represent?
2. Issuer: Who created the token, and how can that identity and authority be verified?
3. Token record: What does the blockchain show about the contract, token ID, address, transfers, and control functions?
4. Metadata and storage: What information or file does the token reference, where is it stored, can it change, and who keeps it available?
5. Rights: What access, license, ownership interest, benefit, or remedy is actually promised in the governing terms?
6. Recognition: Which person, institution, registry, marketplace, or legal system recognizes the claim?
7. Failure conditions: What happens if access credentials are lost, metadata disappears, the issuer fails, the contract contains an error, or the token was created without authority?
8. Alternative: Could an ordinary database, signed document, conventional ticket, or other credential solve the problem more safely or simply?

A careful answer separates established facts from unresolved claims. The token may be one useful piece of evidence. It should not be treated as the complete proof without investigating the rest of the system.

APPLIED SCENARIO: THE TOKENIZED COURSE CERTIFICATE

The following organization and certificate are hypothetical.

LearningBridge Institute offers a 12-week job-readiness course. After a participant completes the reading, written assignments, and final project, the institute creates a non-transferable NFT called LearningBridge Completion Certificate #1842 on a public blockchain.

The token record shows the issuing smart contract, token ID 1842, the date of creation, and the blockchain address that received it. The metadata lists the course title, completion date, and a link to a certificate file stored on the institute's web server. The institute's website says employers can trust every token issued by the contract.

The description leaves important questions unanswered:

» How does an employer verify that the smart contract belongs to LearningBridge Institute?

- What evidence shows that the institute is a legitimate organization and that it followed the stated assessment process?
- How is the blockchain address connected to the correct participant without exposing sensitive personal information?
- Can the metadata or certificate file be changed?
- What happens if the web server stops operating?
- Can the institute correct a misspelled name or revoke a certificate issued by mistake?
- Does non-transferable mean the credential cannot be shared, stolen through lost account access, or displayed by the wrong person?
- Will employers recognize the credential, and what process will they use to verify it?
- Could a signed digital certificate and an ordinary verification database meet the same need with easier recovery and privacy?

Reasoned conclusion: The blockchain record can help show that token 1842 was created by a particular contract and assigned to a particular address. It cannot independently prove the institute's legitimacy, the participant's identity, completion of the course, employer acceptance, or continued availability of the linked certificate. A strong credential system must connect the token record with verified issuer identity, a trustworthy assessment process, durable storage, privacy protections, correction and revocation rules, and a practical verification method.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- A shared token record may make issuance and transfer history easier for different participants to inspect.
- Standard token interfaces may allow compatible wallets and applications to recognize the same type of token.
- Programmable rules may control transferability, access, expiration, or other defined functions.
- A token may support portable membership, ticketing, credential, or record-keeping experiments.
- A public history may help establish when a token was created or moved under the network's rules.

IMPORTANT LIMITATIONS AND RISKS

- The issuer may lack authority or make a false claim.
- The associated file, benefit, physical item, or service may disappear or differ from its description.
- Metadata may change, links may fail, and outside storage may become unavailable.
- Smart-contract errors, stolen credentials, misleading interfaces, or network problems may cause loss or confusion.
- Public records may create privacy risks by connecting activity, identities, memberships, or credentials.
- Token control may not include copyright, title, possession, admission, or other legal rights.
- A copied name, image, symbol, or website can make a fraudulent token look legitimate.
- A specialized token system may add cost and complexity when a database or signed document would work better.
- Legal treatment varies by jurisdiction, claim, agreement, and facts and may change over time.

COMMON MISCONCEPTIONS

- "Non-fungible means the image cannot be copied." The token is distinguishable; an associated file may still be viewed or copied.
- "If it is on a blockchain, it must be authentic." A blockchain can preserve a record of an unauthorized or false token.
- "The token contains the artwork or certificate." Many tokens contain an identifier and metadata that point to a file stored elsewhere.
- "Owning the NFT means owning the copyright." Copyright and token control are separate unless valid terms transfer or license rights.
- "A transfer on the blockchain transfers every real-world right." An outside agreement, registry, law, or institution may control the recognized right.
- "A non-transferable token proves the presenter's identity." A token can be restricted from transfer while the connection between an address and a person remains unverified.
- "Tokenization is always more advanced than a database." A simpler system may provide better privacy, recovery, correction, cost, and accountability.

OFFLINE EXERCISE: WHAT CAN THE CERTIFICATE PROVE?

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Review the LearningBridge Completion Certificate scenario. Create two headings on separate paper:

1. Supported by the token record
2. Requires outside evidence or recognition

Place each statement below under the better heading. If a statement depends on both, explain the boundary.

» Token ID 1842 exists under a particular smart contract.
» A particular blockchain address received the token on the recorded date.
» LearningBridge Institute controls the issuing contract.
» The participant completed the required course work.
» The participant named in the certificate controls the receiving address.
» The certificate file remains available at the metadata link.
» An employer recognizes the credential.
» The institute can correct or revoke a mistaken credential.
» The token has not been transferred under the contract's recorded history.
» The institute had authority to make every statement in the metadata.

THEN ANSWER THESE QUESTIONS:

» What additional evidence would help connect the smart contract to the institute?
» What process could protect the participant's privacy while allowing verification?
» Which correction, revocation, recovery, and storage rules are missing?
» What could a conventional credential database establish more easily?
» Under what conditions might the token add practical value?

Conclude with four or five sentences explaining why the token record should be treated as one part of a credential system rather than the entire proof.

Important limitation of the exercise: The organization, contract, certificate, and token are fictional. The exercise develops reasoning and does not recommend creating or using an NFT.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. What does tokenization mean in this lesson?
   a. Turning every physical object into cryptocurrency
   b. Using a digital token to represent an item, record, right, claim, or form of access
   c. Proving that every tokenized claim is legally enforceable
   d. Storing every associated file directly on a blockchain
2. Which statement best describes a non-fungible token?
   a. It is guaranteed to be valuable because it is unique.
   b. It cannot reference a file stored outside the blockchain.
   c. It is tracked as a distinguishable token, commonly by a contract and token ID.
   d. It automatically transfers copyright in any associated creative work.
3. Which question is most important when evaluating a tokenized certificate?
   a. Does the token have an attractive image?
   b. Did the issuer use a public blockchain?
   c. Who issued the credential, what does the record prove, and what outside evidence supports the claim?
   d. Can the token be discussed on social media?

TRUE OR FALSE

» A blockchain record showing that an address controls an NFT automatically proves that the person controlling the address owns every legal right connected to the referenced item.

SHORT EXPLANATION

» In three or four sentences, explain why a tokenized record and the item or right it represents should be evaluated separately.

SUMMARY AND PRACTICAL TAKEAWAYS

» Tokenization uses a digital token to represent an item, record, right, claim, or form of access.
» Fungible units are interchangeable; non-fungible tokens are tracked separately.
» An NFT's full identity depends on its network, smart contract, and token ID.

- The token record, metadata, referenced item, and governing rights are connected but distinct.
- A blockchain may show creation, address control, and transfer history without proving outside facts.
- Metadata and associated files may be stored off-chain and may change or become unavailable.
- Token control does not automatically include possession, copyright, title, admission, or institutional recognition.
- Authenticity depends on a verified issuer, authority, evidence, and a reliable connection between the token and the claim.
- Public credentials and membership records can create privacy, correction, revocation, and recovery challenges.
- BNB Smart Chain can host token contracts, but the network does not validate every project's claim.
- An ordinary database, signed document, or standards-based credential may solve some problems more simply.

The practical skill is learning to ask what each layer proves. A token can strengthen a record without becoming the item, right, or truth that the record describes.

PROFILE JOURNAL ASSIGNMENT

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

- Define tokenization and non-fungible token in your own words.
- Explain the difference between a token record and the item, service, file, credential, or right it may reference.
- Use the LearningBridge scenario to identify two facts supported by the blockchain record and two claims requiring outside evidence.
- Explain why token control does not automatically transfer copyright or another legal right.
- Identify one possible benefit and two risks or limitations of a tokenized credential.
- Compare the tokenized certificate with an ordinary database or signed digital certificate.
- State when tokenization might add value and when a simpler system might be more responsible.

» Connect this evaluation to the critical-thinking, research, communication, or self-directed-learning skills you are building.

Your response should demonstrate your reasoning. You are not being asked to create a token, open an account, use a wallet, connect to a network or marketplace, disclose personal or financial information, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 11: Tokenization and Non-Fungible Tokens, and the date you completed the entry.

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

1. Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 11 — [date completed].
2. Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
3. Send it to an approved family member or supporter who can enter it on your Profile at PrisonProfessors.org.

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