LESSON 5: WHAT IS A BLOCKCHAIN?

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

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

OPENING GUIDANCE

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

PURPOSE AND ESSENTIAL QUESTION

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

Essential Question:

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

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

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

KEY TERMS

BLOCKCHAIN

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

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

LEDGER

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

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

RECORD

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

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

TRANSACTION

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

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

BLOCK

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

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

NETWORK

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

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

MAIN LESSON

BEGIN WITH THE IDEA OF A LEDGER

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

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

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

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

WHY USE BLOCKS?

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

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

Figure 1. Simplified blockchain structure

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

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

WHY LINK THE BLOCKS?

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

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

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

HOW PARTICIPANTS MAINTAIN A SHARED RECORD

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

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

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

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

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

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

A BRIEF APPLIED EXAMPLE: BNB SMART CHAIN

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

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

WHEN MIGHT A BLOCKCHAIN BE USEFUL?

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

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

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

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

WHAT A BLOCKCHAIN DOES NOT GUARANTEE

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

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

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

APPLIED SCENARIO: A SHARED CREDENTIAL RECORD

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

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

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

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

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

IMPORTANT LIMITATIONS AND RISKS

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

COMMON MISCONCEPTIONS

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

OFFLINE EXERCISE: THE THREE-COPY LEDGER

Estimated time: 15–20 minutes

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

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

SET UP THE LEDGERS

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

VERIFY AND GROUP THE RECORDS

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

CREATE AND RESOLVE A DISAGREEMENT

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

REFLECT ON THE SIMULATION

Write brief notes answering these questions:

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

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

KNOWLEDGE CHECK

MULTIPLE CHOICE

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

TRUE OR FALSE

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

SHORT EXPLANATION

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

SUMMARY AND PRACTICAL TAKEAWAYS

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

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

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

PROFILE JOURNAL ASSIGNMENT

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

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

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

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 5: What Is a Blockchain?, and the date you completed the entry.

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

1. Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 5 — [date completed].
2. Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
3. Send it to an approved family member or supporter who can enter it on your Profile at PrisonProfessors.org.

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