# LESSON 14: HOW A BLOCKCHAIN TRANSACTION WORKS

A Prison Professors Self-Directed Course

**Estimated time:** 65–100 minutes

> *Educational and Safety Boundary: This lesson provides general education about blockchain transactions. It does not provide individualized financial, investment, legal, or tax advice. It does not recommend a wallet, exchange, network, asset, company, or financial product. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson. Do not create, sign, or broadcast a real transaction for any course activity. Never place a real password, private key, seed phrase, authentication code, account number, wallet address, balance, or transaction record in a course response.*

## OPENING GUIDANCE

In earlier lessons, I introduced the public treasury associated with the Prison Professors mission. The independent PP token community made activity connected with that treasury visible on BNB Smart Chain. A person can open a blockchain explorer such as BscScan and see records connected with the published address. That visibility can make a transaction look immediate: a line appears on a screen, a status is displayed, and a balance changes.

Behind that line is a sequence of decisions and network actions. Someone or some authorized system prepares an instruction. The instruction identifies a network, addresses, an action, and a fee. An authorized key signs it. A node receives it. The network checks it. A validator may include it in a block. The transaction may succeed or fail during execution. Confirmations develop, and the network eventually treats the record as final according to its rules.

I want you to understand that sequence because a transaction can be technically valid and still be a bad decision. A correct digital signature does not prove that the signer understood the request. A successful status does not prove that the address belonged to the intended person. A public record does not guarantee that an exchange or another company has credited an account. Technology can verify certain facts, but it cannot replace careful judgment.

The most important work often happens before authorization. A person should slow down, verify the network, examine the destination, understand the proposed action, review the fee, and decide whether the instruction matches the intended purpose.

Once a valid transaction is broadcast and finalized, changing the result may be difficult or impossible.

You can learn this process without using a device or moving an asset. The offline exercise asks you to arrange transaction stages and identify where errors can enter. The purpose is not to practice sending money. The purpose is to practice thinking in sequence.

## PURPOSE AND ESSENTIAL QUESTION

Lesson 14 traces a blockchain transaction from preparation through authorization, network processing, confirmation, and final recordkeeping. It separates actions taken by a user or application from actions taken by nodes, validators, and the network.

**Essential Question:**

- Why do verification and patience matter before and after a person authorizes a blockchain transaction?

## LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- Sequence the major stages of a blockchain transaction.
- Explain the roles of addresses, digital signatures, fees, nodes, validators, confirmations, and finality.
- Distinguish preparation, authorization, broadcast, validation, execution, inclusion, confirmation, and finality.
- Identify common reasons a transaction may be delayed, rejected, fail during execution, or succeed in an unintended way.
- Describe precautions that reduce address, network, fee, contract, and counterparty errors.

## KEY TERMS

### DIGITAL SIGNATURE

**Definition:** Cryptographic evidence created with a private key to authorize a specific digital message or transaction. A network can use the signature to check that the transaction was authorized by the key connected with the sending account. A valid signature does not prove the signer's identity, wisdom, ownership rights, or understanding of the transaction.

**Sample sentence:** The digital signature showed that the transaction was authorized by the required key, but it did not show why the signer approved it.

### TRANSACTION FEE

**Definition:** A charge paid for network resources used to process a transaction. On many networks, the fee depends on the work requested, network demand, and fee settings. The fee is normally paid in the network's native asset, even when the transaction involves another token.

**Sample sentence:** The token transfer required a transaction fee in the network's native asset.

### BROADCAST

**Definition:** To send a signed transaction to a network node so that it can be checked and relayed to other nodes. Broadcasting submits the instruction; it does not guarantee inclusion, success, or finality.

**Sample sentence:** After the wallet broadcast the signed transaction, the instruction entered the network's pending process.

### VALIDATION

**Definition:** The process of checking whether a transaction follows network rules. Checks may include the signature, account sequence, available balance, fee requirements, transaction format, and rules governing the requested action.

**Sample sentence:** Validation rejected the instruction because it did not meet the network's requirements.

### CONFIRMATION

**Definition:** Evidence that a transaction has been included in a block accepted by the network. Additional blocks or network votes may increase confidence that the record will remain part of the accepted history. The meaning of a confirmation differs by network.

**Sample sentence:** The organization waited for the required confirmation standard before updating its records.

### FINALITY

**Definition:** The point at which a blockchain's rules provide strong assurance that an accepted transaction will not be reversed. Different networks reach or describe finality in different ways and on different schedules.

**Sample sentence:** The public record showed the transaction in a block, but the team followed its policy and waited for finality before relying on it.

## MAIN LESSON

### A TRANSACTION IS A SIGNED INSTRUCTION

People sometimes speak as if a digital asset travels through the internet like a package moving through the mail. That description can mislead. On a blockchain, a transaction is better understood as an instruction asking the network to update its shared state.

A simple instruction might ask the network to reduce the recorded balance associated with one account and increase the balance associated with another. A more complex instruction might call a function in a smart contract. It might transfer a token, record an approval, exchange one asset for another, vote in a governance process, or carry out another programmed action.

The instruction normally contains several fields. The exact fields differ by network and transaction type, but they may include:

- The network on which the transaction is intended to operate.
- A sending account or address.
- A destination address, such as another account or a smart contract.
- An amount or requested function.
- Data that tells a smart contract what action is requested.
- A transaction sequence or nonce that helps prevent duplication and preserves order.
- A limit and price for network computation or other fee information.
- A digital signature authorizing the completed instruction.

Some information can be prepared by a wallet or application. The user may see only a summary. That convenience creates a responsibility: the summary should be checked, and any unclear request should be treated cautiously. Signing an instruction that cannot be understood is sometimes called blind signing. A careful person does not assume that a button labeled “confirm” describes every effect.

### STAGE 1: PREPARE THE INSTRUCTION

Preparation begins before a private key is used. A person, organization, wallet, exchange, or application assembles the proposed transaction.

At this stage, the preparer should identify:

- The correct blockchain network.
- The correct asset or smart contract.
- The intended destination address.
- The amount or requested action.
- The estimated transaction fee and the native asset needed to pay it.
- Any service fee or withdrawal fee charged outside the blockchain fee.
- Any memo, destination tag, reference, or additional information required by the receiving service.

These details matter because the same-looking address may be used on more than one compatible network, while an exchange or service may support only one route. A transaction can succeed on the selected network and still fail to produce the intended result at the receiving service. That is not necessarily a network failure. It may be a network-selection or counterparty problem.

Fees also require care. On BNB Smart Chain, BNB is the native asset used to pay transaction fees. A person sending another token may still need enough BNB for the fee. A displayed estimate can change with network conditions or with the complexity of a smart-contract action. An estimate is not a promise.

#### STAGE 2: REVIEW BEFORE AUTHORIZATION

Review is the last ordinary opportunity to catch an error before signing. The reviewer should compare the proposed instruction with an independent, trusted source of information.

A careful review asks:

- Am I using the intended network?
- Does the destination match the verified address or service instructions?
- Is the asset the intended asset, including the correct token contract when relevant?
- Is the amount correct, including the decimal placement?
- Does the application describe the action clearly?
- Am I approving a transfer, a token allowance, a contract interaction, or something else?
- Is the fee reasonable for the proposed action and current conditions?
- Am I being pressured to act quickly or keep the transaction secret?

Copying and pasting can reduce typing errors, but it does not remove risk. Malicious software can replace a copied address. A familiar beginning and ending

are not always enough to establish that a long address is correct. When circumstances permit, a person should compare the complete address or use a trusted address-book process. Organizations should use written verification and approval rules rather than memory alone.

#### STAGE 3: AUTHORIZE WITH A DIGITAL SIGNATURE

After review, the authorized key holder may sign the transaction. The signature is created from the transaction data and the private key. The private key should remain secret; the signature can be shared with the network.

The signature performs an important but limited job. It allows the network to verify that the required key authorized that exact transaction data. If the transaction data changes after signing, the signature will no longer match.

The signature does not answer every question. It does not prove that the signer:

- Is the legal owner of the asset.
- Understood the contract interaction.
- Was free from pressure or deception.
- Used a secure device.
- Chose the correct network or address.
- Followed an organization's internal policy.
- Made a financially wise decision.

This distinction connects with Lesson 13. Custody determines who can authorize. Transaction discipline determines how that authority is used.

#### STAGE 4: BROADCAST TO THE NETWORK

The signed transaction is sent to a node. The node performs initial checks and may relay the transaction to other nodes. On many networks, valid pending transactions wait in a transaction pool, sometimes called a mempool, until a validator or block producer selects them.

Broadcasting is not the same as completing. A wallet or service may display a transaction identifier, often called a transaction hash, soon after submission. That identifier helps people locate or discuss the transaction. It is not proof that the transaction has been included in a block, executed successfully, credited by a receiving company, or finalized.

A transaction may remain pending because network demand is high, the offered fee is unattractive, a required earlier transaction from the same account is still pend-

ing, a node has not relayed it widely, or a service has not actually broadcast the instruction. Some systems allow a pending transaction to be replaced with another transaction using the same sequence number and a different fee. The details vary, so a person should follow verified instructions from the relevant network or service rather than improvising.

### STAGE 5: VALIDATE, EXECUTE, AND INCLUDE

Nodes and validators apply network rules. A transaction may be rejected before inclusion if its format, signature, sequence, balance, or fee does not meet those rules. A rejected transaction does not become part of the accepted blockchain history.

A validator may select a valid pending transaction and place it in a proposed block. For a simple transfer, execution may update balances. For a smart-contract interaction, the network executes the contract code with the supplied data.

Execution can succeed or fail. A contract may reject the request because a condition was not met. The transaction may run out of the allowed computational resource. An attempted token transfer may fail because the sending account lacks the token balance or permission required by the contract.

An included but failed transaction can still consume a transaction fee because the network performed work. On Ethereum-compatible networks, including BNB Smart Chain, the exact fee rules depend on the network and transaction. This is one reason a status of "failed" should not be confused with "nothing happened." The intended state change may have been reversed, while a fee may still have been charged and a public record may still exist.

### STAGE 6: READ THE RECEIPT AND CONFIRMATION STATUS

After inclusion, the network produces a transaction receipt or equivalent record. A block explorer may display information such as:

- The transaction hash.
- The block containing the transaction.
- The sending and destination addresses.
- The network fee.
- Whether execution succeeded or failed.
- Token-transfer events or other contract logs.
- The number of later blocks or confirmations.

An explorer translates network data into a readable page. It is useful, but it is not the blockchain itself, and its labels can be misunderstood. A "success" status generally

means the network executed the requested instruction without a protocol-level failure. It does not prove that the recipient was correct, that an off-chain company credited the right account, that a token has value, or that the transaction served the mission.

For a transaction involving an exchange, custodian, merchant, or another service, two records may matter. The blockchain records the on-chain event. The company keeps its own account records and may require a memo, supported network, minimum amount, identity review, or a certain number of confirmations. A blockchain success does not force the company's internal system to credit an account immediately.

### STAGE 7: WAIT FOR FINALITY AND RECONCILE THE RECORDS

Networks use different methods to decide when an accepted block should be treated as final. Some rely on additional blocks, some use validator votes, and some combine methods. BNB Smart Chain uses validator consensus and a fast-finality process. Exact validator counts, block times, and finality timing can change through network upgrades, so they should be checked against current official documentation before publication or operational use.

Patience matters between first inclusion and finality. A careful policy defines what evidence is sufficient before a person or organization relies on a transaction. That policy may depend on the network, value, risk, counterparty, and legal or organizational requirements.

After finality, responsible recordkeeping should reconcile several questions:

- Did the intended transaction reach the intended network and address?
- Did execution succeed?
- What fee was charged?
- Did any related token event occur?
- Did the receiving service or internal ledger record the result?
- Did the transaction follow the organization's approval and mission rules?

Finality answers a blockchain-history question. It does not answer every accounting, legal, tax, ownership, or ethical question.

## APPLIED SCENARIO: A COMMUNITY TREASURY TRANSACTION

The independent PP token community has used BNB Smart Chain and a public treasury address associated with the Prison Professors mission. Imagine that a community tracker reports a new community-generated fee transaction connected with that treasury. This simplified teaching scenario does not describe or verify every rule in the token's smart contract, and it does not promote the token or any digital asset.

An observer might see a new entry on BscScan and say, "The donation is complete." A more careful analysis separates the stages and the claims.

**Preparation:** A wallet, contract, or application assembled a transaction on BNB Smart Chain. The instruction identified addresses, data or value, and a fee paid in the network's native asset.

**Authorization:** An authorized key produced the required digital signature. If a smart contract initiated part of the process, a prior signed transaction may have called the contract. The public record does not reveal the private key.

**Broadcast and validation:** A node received and relayed the signed instruction. Network participants checked that it followed BNB Smart Chain rules.

**Execution and inclusion:** A validator included the transaction in a block. The network executed the requested action and created a receipt showing success or failure.

**Confirmation and finality:** Later network acceptance increased confidence that the record would remain in the chain's history.

**Reconciliation:** Observers could compare the public record with the published treasury address and community report. That comparison could support a limited statement about on-chain activity. It would not, by itself, prove the complete custody arrangement, every contract rule, donor identity, legal ownership, future value, internal accounting treatment, or mission compliance.

This example connects technical discipline with credibility. If I describe the public treasury, I should state what the blockchain evidence supports and avoid claiming more. Participants can practice the same habit in their own work: identify the evidence, trace the sequence, and separate a verified fact from an assumption.

Delays, Failures, and Successful Mistakes

Not every problem has the same meaning. A careful learner distinguishes four categories.

#### DELAYED OR PENDING

The signed transaction has been submitted but has not yet reached the required inclusion or confirmation status. Possible causes include network demand, fee settings, sequence conflicts, node problems, or a service delay.

#### REJECTED BEFORE INCLUSION

The network or submitting service refuses the transaction before it enters an accepted block. Possible causes include an invalid signature, incorrect format, insuf-

ficient balance for the amount and fee, an invalid sequence, or fee settings that do not meet network requirements.

#### INCLUDED BUT FAILED DURING EXECUTION

The transaction enters a block, but the requested state change does not complete. A smart contract may reject the action, or the transaction may exhaust its computational allowance. The public record may show failure, and a network fee may still be charged for work performed.

#### TECHNICALLY SUCCESSFUL BUT UNINTENDED

The network executes exactly what was signed, but the signer chose the wrong address, wrong network, wrong token, wrong amount, harmful contract approval, or dishonest counterparty. The blockchain may show success even though the human purpose failed.

That final category is especially important. Network validation checks protocol rules. It does not guarantee good judgment.

## BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

#### BENEFITS OF A TRACEABLE TRANSACTION PROCESS

- A digital signature can link authorization to a specific key without revealing the private key.
- Shared network rules allow independent nodes to check the transaction.
- A transaction hash and public record can support tracking and reconciliation.
- Confirmations and finality provide increasing assurance that accepted history will remain stable.
- Organizations can use written approval and verification procedures around the technical process.

#### IMPORTANT LIMITATIONS AND RISKS

- A valid signature can authorize a harmful or misunderstood instruction.
- An address usually does not identify a human being by itself.
- Transactions may be irreversible after finality.
- Fees may change, and failed execution may still consume a fee.
- Smart-contract actions may have effects that a simple wallet summary does not explain.
- A blockchain record may not match an exchange, merchant, court, accounting system, or organization's internal record.

» A public transaction can expose patterns that affect privacy.
» Compatible-looking networks and tokens can create routing and identification errors.

### COMMON MISCONCEPTIONS

» "Broadcast means complete." Broadcast means that a signed instruction was submitted to a node; it may still be pending, rejected, replaced, or dropped.
» "A transaction hash proves success." A hash identifies a transaction. Its receipt and status must still be checked.
» "One confirmation always means final." Networks define confirmation and finality differently.
» "Success means the intended person received the asset." Network success proves execution under protocol rules, not human identity or intent.
» "A failed transaction costs nothing." An included transaction that fails during execution may still consume a fee.
» "The fee is paid in whatever token I am sending." Many networks require the fee in their native asset.
» "The blockchain will correct a wrong address." A valid transaction can succeed at an unintended address.
» "A block explorer is customer support." An explorer displays public data; it generally cannot reverse a transaction or control an account.

## OFFLINE EXERCISE: PUT THE TRANSACTION IN ORDER

**Estimated time:** 25–30 minutes

**Materials:** Separate paper and a pencil.

The eight cards below are deliberately out of order. Do not create an account or perform a real transaction. On separate paper, write the letters in the order that best represents a typical blockchain transaction.

### TRANSACTION-STAGE CARDS

**Card A:** A validator includes the transaction in a block and the network executes the requested action.

**Card B:** The preparer or reviewer checks the network, address, asset, amount, action, and estimated fee.

**Card C:** The authorized key creates a digital signature for the completed transaction data.

**Card D:** A node receives the signed transaction and relays it to the network.

**Card E:** The accepted record gains confirmations and reaches the network's finality standard.

**Card F:** A wallet, application, contract, or service assembles the proposed transaction fields.

**Card G:** Network participants check the signature, sequence, balance, fee, format, and other protocol rules.

**Card H:** A receipt or explorer record shows the block, fee, and success or failure status.

After arranging the cards, complete these tasks:

1. Identify one error that could enter during preparation or review.
2. Identify one risk that a valid digital signature cannot prevent.
3. Explain why broadcasting does not prove success.
4. Explain the difference between a rejected transaction and an included transaction that fails during execution.
5. Explain why a technically successful transaction may still fail its human purpose.
6. Identify what an organization should verify when reconciling an on-chain transaction with its internal records.
7. Write one sentence explaining why patience matters after the first confirmation.

**Important limitation of the exercise:** The cards describe a simplified, typical process. Networks, layers, wallets, custodians, smart contracts, and services may combine, reorder, or label stages differently. The exercise teaches reasoning, not an operational procedure.

## KNOWLEDGE CHECK

### MULTIPLE CHOICE

1. What does a digital signature establish most directly?
   a. That the signer made a wise decision
   b. That the required private key authorized the specific transaction data
   c. That the destination belongs to the intended person
   d. That the transaction is already final
2. Which statement best describes broadcast?

a. The transaction has been submitted to a network node, but inclusion and success are not guaranteed
b. The transaction has reached finality
c. The recipient's company has credited an internal account
d. The fee has been refunded

3. Which situation can appear as successful on-chain while still failing the signer's purpose?
   a. A node rejects a transaction with an invalid signature
   b. A wallet has not yet assembled an instruction
   c. A valid transaction sends an asset to the wrong address
   d. A learner completes the exercise on paper

#### TRUE OR FALSE

» If a transaction is included in a block but fails during smart-contract execution, a network fee may still be charged for the work performed.

#### SHORT EXPLANATION

» In three or four sentences, explain why a transaction hash and a success status do not prove that every human, business, legal, or ethical purpose was satisfied.

### SUMMARY AND PRACTICAL TAKEAWAYS

» A blockchain transaction is a signed instruction asking a network to update its shared state.
» Preparation identifies the network, address, asset, amount, action, and fee.
» Review is the last ordinary opportunity to catch many errors before authorization.
» A digital signature proves authorization by a key, not identity, wisdom, ownership, or freedom from deception.
» Broadcast submits a signed transaction to a node; it does not guarantee inclusion, success, or finality.
» Validation checks protocol rules such as signature, sequence, balance, format, and fee requirements.
» A validator may include a transaction in a block and execute the requested action.
» A rejected transaction, a pending transaction, an included failure, and a successful mistake are different outcomes.

- An included transaction that fails during execution may still consume a transaction fee.
- A transaction hash helps locate a transaction but does not prove success.
- Confirmation and finality have network-specific meanings.
- A blockchain success does not guarantee that an exchange, merchant, or other counterparty has updated its own records.
- BNB Smart Chain uses BNB for transaction fees, including transactions involving other tokens.
- The Prison Professors community treasury example shows how public evidence can support a limited claim without proving every private or off-chain fact.
- Verification, patience, reconciliation, and honest communication strengthen credibility.
- No course exercise requires a real account, wallet, asset, or transaction.

**The practical lesson is simple:** slow down before signing, identify what each stage proves, and do not confuse technical success with complete human success.

### PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Write in the first person, as part of the Profile you are building. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- Explain in your own words what a blockchain transaction is.
- Sequence the major stages from preparation through finality.
- Describe what a digital signature proves and what it does not prove.
- Explain why a transaction hash, confirmation, and finality are different.
- Identify one address or network error and one fee or smart-contract error that careful review may reduce.
- Explain the difference between a rejected transaction, an included failure, and a technically successful mistake.
- Use the Prison Professors community treasury example to distinguish on-chain evidence from custody, accounting, ownership, or mission claims.
- Explain why verification and patience matter before and after authorization.
- Connect transaction discipline with responsibility, credibility, preparation, or trust.

Your response should demonstrate reasoning. Do not create, sign, or broadcast a transaction. Do not include any real password, private key, seed phrase, authentication code, account number, wallet address, balance, transaction hash, or transaction detail.

## SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 14: How a Blockchain Transaction Works, and the date you completed the entry.

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

1. Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 14 — [date completed].
2. Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
3. Send it to an approved family member or supporter who can enter it on your Profile at PrisonProfessors.org.

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

### TECHNICAL AND SAFETY CONTEXT REVIEWED JULY 22, 2026.


1. Prison Professors. Understanding Web3 — Course Blueprint, Version 1.1, July 2026; Lesson 12: Wallets, Addresses, Keys, and Seed Phrases, approved Draft Version 0.1; Lesson 13: Custody and Self-Custody, approved Draft Version 0.2; and project direction I supplied for this course. Controlling sources for the lesson requirements, first-person voice, community-treasury case, offline design, submission process, and sensitive-information boundaries.
2. Ethereum.org. "Transactions," updated March 12, 2026; accessed July 22, 2026. Used for the signed-instruction model, transaction fields, broadcast, pending pool, validator inclusion, and lifecycle explanation. https://ethereum.org/developers/docs/transactions/
3. Ethereum.org. "Ethereum Gas and Fees: Technical Overview," updated June 24, 2026; accessed July 22, 2026. Used for computational-resource explanations, fee purpose, unused gas, and the distinction between rejection before inclusion and failure during execution. https://ethereum.org/developers/docs/gas/

4. BNB Chain. “BNB Smart Chain Introduction” and “BNB Smart Chain Quick Guide”; accessed July 22, 2026. Used for BNB Smart Chain’s validator-based processing, fast-finality context, Ethereum compatibility, and BNB as the native transaction-fee asset. Exact network parameters are time-sensitive and should be reverified before publication. https://docs.bnbchain.org/bnb-smart-chain/introduction/ and https://docs.bnbchain.org/bnb-smart-chain/developers/quick-guide/