Topic 3.3: Wallets, Transactions & The UX Gap

User Experience Challenges in Blockchain

Joerg Osterrieder

Digital Finance

2025

Learning Objectives

By the end of this topic, you will be able to:

1. **Define** what a cryptocurrency wallet actually is and what it stores
2. **Compare** different wallet types (custodial, hot, cold, hardware)
3. **Explain** the anatomy of a blockchain transaction
4. **Calculate** transaction fees using gas economics
5. **Identify** the user experience gap between traditional banking and crypto
6. **Recognize** common user errors and their consequences
7. **Evaluate** current solutions for improving crypto UX

Why This Matters

Understanding wallets and transactions is essential for anyone working in digital finance – these are the fundamental interfaces between users and blockchain technology.

Prerequisites: A Quick Recap on Keys

From Topic 3.1: Cryptographic Foundations

Private Key

- A secret 256-bit random number (a number so large it's practically impossible for anyone else to guess)
- Only you should know it
- Used to *sign* transactions
- Proves you authorize spending
- If lost: funds gone forever

Public Key & Address

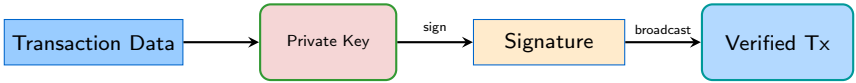
- Derived from private key
- Can be shared with anyone
- Your "account number"
- Others send funds here
- Safe to share publicly

Key insight: Private key → Public key is one-way (cannot reverse)

How Transactions Get Authorized

A **digital signature** proves that:

1. The owner of the private key authorized this exact transaction
2. The transaction hasn't been modified since signing
3. The signer cannot deny having signed it (non-repudiation)

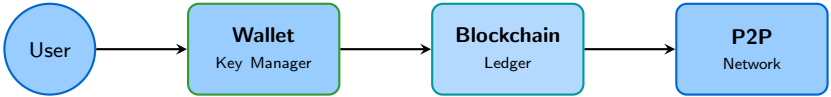


Anyone can verify a signature using the public key, but **only the key holder** can create valid signatures.

Connection to Wallets

A wallet's primary job is to securely store private keys and use them to sign transactions.

From Theory to Practice: How Users Interact



Key insight: Users never interact with the blockchain directly.
The **wallet** is the interface – it manages keys, signs transactions, and broadcasts them to the network.

Common Misconception

Wallets don't "store" cryptocurrency. The blockchain stores balances.
Wallets store *keys* that prove you can spend those balances.

What Is a Wallet, Really?

A wallet is a key management tool
It does three things:

1. **Stores private keys** (securely, hopefully)
2. **Signs transactions** using those keys
3. **Broadcasts transactions** to the network

It does NOT:

- Store cryptocurrency
- Connect you to a bank
- Know your identity
- Require permission to create

Wallet Contents

Private Key 1

0x7a2b...secret

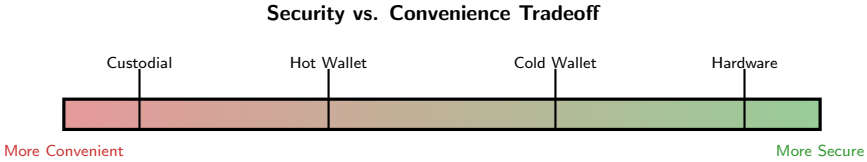
Address 1: 0x9c4d...

Address 2: 0xf3e8...

Balance: 1.5 ETH

(queried from blockchain)

Types of Wallets: A Spectrum of Tradeoffs



Type	Key Control	Example	Risk
Custodial	Exchange holds keys	Coinbase, Binance	Exchange hack
Hot Wallet	You hold, online	MetaMask	Malware, phishing
Cold Wallet	You hold, offline	Paper wallet	Physical loss
Hardware	You hold, secure chip	Ledger, Trezor	Device failure

Custodial Wallets: Someone Else Holds Your Keys

Definition: A **custodial wallet** is one where a third party (typically an exchange) controls the private keys on your behalf.

How It Works

1. You create an account with an exchange
2. Exchange generates keys for you
3. You see a balance in your account
4. When you "send," exchange signs
5. You never see the private key

Examples:

- Coinbase
- Binance
- Kraken
- Crypto.com

Pros and Cons

Advantages:

- Easy to use (like a bank app)
- Password recovery possible
- Customer support available
- Fiat on/off ramps

Disadvantages:

- You don't control your keys
- Exchange can freeze your funds
- Exchange can be hacked
- May require KYC/identity

Non-Custodial Wallets: You Control Your Keys

Definition: A **non-custodial wallet** (or self-custody wallet) is one where only you control the private keys.

How It Works

1. You generate keys yourself
2. Keys stored on your device
3. You sign all transactions
4. No account required
5. No permission needed

Examples:

- MetaMask (browser extension)
- Trust Wallet (mobile)
- Electrum (Bitcoin)
- Ledger/Trezor (hardware)

Pros and Cons

Advantages:

- Full control of your funds
- No counterparty risk
- Censorship resistant
- Privacy (no KYC)

Disadvantages:

- You are fully responsible
- Lose keys = lose funds
- No customer support
- Steeper learning curve

"Not your keys, not your coins"
A fundamental principle of cryptocurrency ownership

Hot vs. Cold Wallets: Internet Connectivity

Key Question: Is your wallet connected to the internet?

Hot Wallet
(Internet-connected)

- Keys stored on online device
- Computer, phone, browser
- Ready for immediate use
- Good for daily transactions
- Vulnerable to hackers

Analogy: Cash in your pocket – convenient for daily spending

Cold Wallet
(Offline)

- Keys never touch internet
- Paper, hardware device, air-gapped computer
- Requires extra steps to use
- Good for long-term storage
- Much more secure

Analogy: Money in a safe deposit box – secure for savings

Best Practice

Use both: hot wallet for daily use (small amounts), cold storage for savings (large amounts).

Hardware Wallets: The Gold Standard for Security

Definition: A **hardware wallet** is a dedicated physical device that stores private keys offline and signs transactions securely.

How It Works

1. Keys generated and stored on device
2. Keys *never* leave the device
3. Transaction data sent to device
4. Device signs internally
5. Only signature returned to computer

Popular Hardware Wallets:

- Ledger Nano (S/X)
- Trezor (One/Model T)
- GridPlus Lattice1
- Keystone Pro

Security Features

- Secure element chip
- PIN code protection
- Physical confirmation button
- Display shows transaction details
- Recovery phrase backup

Typical Cost: $50–$200

Recommended for:
Anyone holding ¿$1,000 in crypto

Seed Phrases: Your Master Backup

Definition: A **seed phrase** (or recovery phrase) is a list of 12-24 words that can regenerate all your private keys.

```
abandon ability able about above absent absorb abstract absurd abuse access accident
```

This 12-word phrase encodes your entire wallet. Anyone with these words controls your funds.

How It Works (BIP-39)

- 2,048 possible words
- 12 words = 128 bits entropy
- 24 words = 256 bits entropy
- Mathematically generates keys
- One phrase → unlimited addresses

Critical Security Rules

- NEVER share with anyone
- NEVER type into a website
- NEVER store digitally
- Write on paper or metal
- Store in multiple secure locations

Lose your seed phrase + lose your device = permanently lose all funds

Custodial vs. Non-Custodial: Direct Comparison

Custodial (Exchange) Wallet
You → Exchange → Blockchain

- Easy to use
- Password recovery possible
- Fiat on/off ramps
- You don't control keys
- Exchange can freeze funds
- Exchange can be hacked

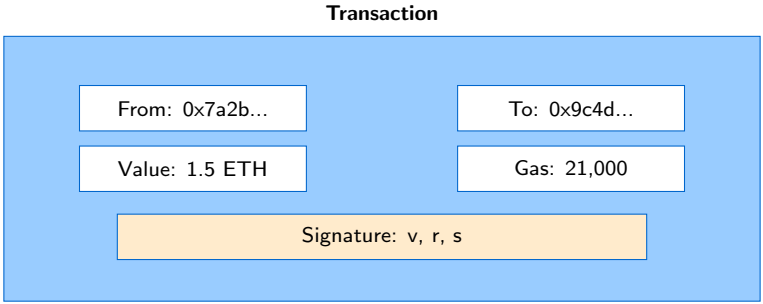
Non-Custodial (Self-Custody)
You → Your Wallet → Blockchain

- Full control
- No counterparty risk
- Censorship resistant
- You are responsible
- Lose keys = lose funds
- No customer support

FTX Collapse (2022)
$8 billion in customer funds lost when exchange failed.
Customers using custodial wallets had no recourse.

What Is a Blockchain Transaction?

Definition: A **transaction** is a signed message that transfers value or triggers computation on a blockchain.



Key Components:

- **From:** Sender's address (derived from signature)
- **To:** Recipient's address
- **Value:** Amount to transfer
- **Gas:** Computational budget
- **Signature:** Cryptographic proof of authorization

Anatomy of a Blockchain Transaction

Ethereum Transaction Structure

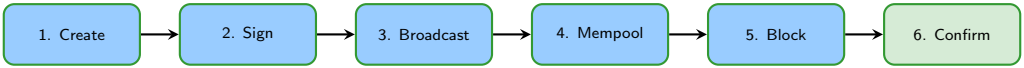
Field	Example Value	Purpose
From	0x7a2b...9f3c	Sender's address
To	0x9c4d...e8f2	Recipient's address
Value	1.5 ETH	Amount to transfer
Nonce	42	Transaction count (prevents replay)
Gas Limit	21,000	Maximum computation units
Gas Price	50 gwei	Price per gas unit (see frame 18)
Signature	v, r, s	Proves authorization

The signature covers ALL fields above it – proving the sender authorized *this exact transaction*.

What is a Nonce?

The nonce is a counter that tracks how many transactions you've sent. It prevents attackers from replaying old transactions and ensures transactions are processed in order.

Transaction Lifecycle: From Creation to Confirmation



1. **Create:** Wallet builds transaction with recipient, amount, gas
2. **Sign:** Private key creates digital signature
3. **Broadcast:** Transaction sent to network nodes
4. **Mempool:** Waits in "waiting room" for inclusion
5. **Block:** Miner/validator includes in a block
6. **Confirm:** Block added to chain; more blocks = more confirmations

Mempool Definition

The **mempool** (memory pool) is where valid but unconfirmed transactions wait before being included in a block. Each node maintains its own mempool.

Understanding Gas: The Cost of Computation

What is Gas?

- Unit measuring computational work
- Each operation has a gas cost
- Simple transfer: 21,000 gas
- Smart contract call: varies (100K+)

Gas Economics

Analogy: Gas limit = max fuel in tank; Gas price = cost per gallon

$$\text{Fee} = \text{Gas Used} \times \text{Gas Price}$$

Example:

- Gas used: 21,000
- Gas price: 50 gwei (explained in detail on next frame)
- Fee = 21,000 × 50 gwei = 0.00105 ETH

Why Gas Exists

1. Prevents infinite loops
2. Compensates validators
3. Prioritizes transactions
4. Allocates scarce block space

Network Congestion

High demand → Higher gas prices → Higher fees

(Supply and demand)

Gas prices fluctuate wildly – from cents to hundreds of dollars per transaction

Gas Price Units: Gwei Explained

Definition: Gwei (giga-wei) is the standard unit for measuring gas prices on Ethereum.

Think of it like cents to dollars, but with more decimal places:
Wei is the smallest unit (like a penny's fraction), and ETH is the whole unit (like a dollar).

Unit	Value in Wei	Value in ETH
Wei	1	0.000000000000000001 ETH
Gwei	1,000,000,000	0.000000001 ETH
ETH	1,000,000,000,000,000,000	1 ETH

Typical Gas Prices:

- **Low activity:** 10-20 gwei
- **Normal activity:** 30-50 gwei
- **High congestion:** 100-200+ gwei
- **NFT drop/DeFi rush:** 500+ gwei

Quick Calculation

At 50 gwei, a simple ETH transfer costs: $21,000 \times 50 = 1,050,000$ gwei $= 0.00105$ ETH
If ETH = \$2,000, that's about \$2.10 per transaction.

EIP-1559: Modern Ethereum Fee Structure

Ethereum changed its fee system in 2021 to make costs more predictable.

EIP = Ethereum Improvement Proposal – a formal suggestion to change Ethereum's rules, similar to a bill in parliament.

Since August 2021, Ethereum uses a two-part fee system:

Base Fee

- Algorithmically determined
- Adjusts based on congestion
- Burned (not paid to validators)
- Creates deflationary pressure

Priority Fee (Tip)

- Optional tip to validator
- Incentivizes faster inclusion
- Paid to validator
- Higher tip = faster confirmation

Total Fee Formula

$$\text{Fee} = (\text{Base Fee} + \text{Priority Fee}) \times \text{Gas Used}$$

Example: $(20 + 2) \times 21,000 = 462,000$ gwei $= 0.000462$ ETH

Benefit: More predictable fees. Base fee adjusts smoothly instead of wild bidding wars.

Definition: A **confirmation** occurs each time a new block is added after the block containing your transaction.

Blockchain	Recommended	Time
Bitcoin	6 confirmations	$\sim$60 minutes
Ethereum (PoS)	2 epochs (finality)	$\sim$15 minutes
Ethereum (small amounts)	12 confirmations	$\sim$3 minutes

Why wait? More confirmations = harder to reverse. Protects against chain reorganizations.

Two Models: UTXO vs. Account-Based

How does the blockchain track who owns what?

Two different approaches: think of UTXO like having specific bills in your wallet (you can't tear a $10 bill in half), vs. an account balance like a bank (just a number that goes up and down).

UTXO Model (Bitcoin)
Unspent Transaction Outputs

- Balance = sum of unspent outputs
- Must spend entire UTXO
- Creates "change" outputs
- Better for privacy
- Better for parallelization

Analogy: Cash bills
You can't tear a $10 bill

Account Model (Ethereum)
Like a bank account

- Balance stored directly
- Can send any amount
- No change needed
- Simpler to understand
- Better for smart contracts

Analogy: Bank account
Balance adjusted up/down

UTXO Example

Alice has 0.5 BTC (one UTXO). To send 0.3 BTC: she spends the entire 0.5 BTC UTXO, sends 0.3 BTC to Bob, and 0.2 BTC back to herself as "change."

The User Experience Gap

What crypto asks users to understand:

Traditional Banking

- Username and password
- "Forgot password?" link
- Customer support
- FDIC insurance
- Fraud protection
- Clear error messages

Forgiving of mistakes

Cryptocurrency

- 24-word seed phrase
- Lose phrase = lose everything
- No customer support
- No insurance (usually)
- Irreversible transactions
- Cryptic error: "insufficient gas"

Unforgiving of mistakes

The UX Problem

Crypto's security model requires users to be their own bank.
Most people don't want that responsibility.

Common User Errors (And Their Consequences)

Error	Consequence	Recovery?
Lost seed phrase	Permanent loss of funds	No
Sent to wrong address	Funds gone forever	No
Wrong network (ETH to BSC)	Funds stuck/lost	Sometimes
Insufficient gas	Transaction fails	Yes, retry
Approved malicious contract	Wallet drained	No
Phishing attack	Keys stolen	No
Didn't verify contract	Funds stolen	No

Scale of the problem:

- $3.8 billion lost to crypto hacks in 2022 (Chainalysis)
- Estimated 20% of Bitcoin permanently inaccessible (lost keys)
- Phishing remains the #1 attack vector

Improving Crypto UX: Current Efforts

Technical Solutions

- **Account abstraction:** Smart contract wallets with recovery
- **Social recovery:** Trusted friends can help recover
- **Multi-sig:** Require multiple keys to transact
- **Hardware wallets:** Secure key storage
- **ENS names:** Human-readable addresses (e.g., alice.eth)

UX Improvements

- **Transaction simulation:** Show what will happen before signing
- **Clear warnings:** "This will drain your wallet"
- **Gas estimation:** Show fees in dollars
- **Address books:** Saved, verified addresses
- **Better error messages:** Human-readable explanations

The Goal

Make self-custody as easy as using a bank app, without sacrificing security or decentralization.

Hands-On Exercise: Blockchain Transaction Analysis

NB07: Blockchain Transactions

In the accompanying Jupyter notebook, you will:

1. **Build a transaction** from scratch with all required fields
2. **Calculate gas fees** for different types of operations
3. **Compare UTXO vs. Account models** through examples
4. **Analyze transaction lifecycle** from creation to confirmation
5. **Simulate fee markets** under different network conditions

Learning Goals

- Understand transaction structure at a technical level
- Practice fee calculations (gas units $\times$ gas price)
- See how the mempool works
- Compare Bitcoin and Ethereum transaction models

Hands-On: Code Preview

Example from NB07: Building a Transaction

```python
# Transaction structure (simplified)
transaction = {
    "from": "0x742d35Cc6634C0532925a3b844Bc9e7595f8aB12",
    "to": "0x8Ba1f109551bD432803012645Ac136ddd64DBA72",
    "value": 1.5,  # ETH
    "gas_limit": 21000,  # Standard transfer
    "gas_price": 50,  # Gwei
    "nonce": 42
}

# Calculate transaction fee
fee_gwei = transaction["gas_limit"] * transaction["gas_price"]
fee_eth = fee_gwei / 1e9
print(f"Transaction fee: {fee_eth} ETH")
```

Output: Transaction fee: 0.00105 ETH

Try it: Open NB07 and experiment with different gas prices!

Discussion: Choosing the Right Wallet

Scenario Analysis

Consider these users – which wallet type would you recommend?

1. **Alice** is new to crypto and wants to buy $100 of Bitcoin to hold for years.
2. **Bob** is a DeFi power user who interacts with smart contracts daily.
3. **Carol** runs a crypto hedge fund and manages $10 million in assets.
4. **Dave** lives in a country with capital controls and needs censorship resistance.

Discussion Questions

- What factors should each person prioritize?
- How does the amount at stake affect the choice?
- When does convenience outweigh security (and vice versa)?

Discussion: Transaction Fee Strategies

When to pay more, when to pay less

Scenario 1: Urgent Transfer

- You need to deposit ETH to an exchange to sell before price drops
- Network is congested
- Current gas: 100 gwei
- What gas price do you set?

Scenario 2: Non-Urgent Transfer

- You're moving crypto to cold storage
- No time pressure
- Current gas: 50 gwei
- What gas price do you set?

Advanced Strategies:

- **Wait for low traffic:** Weekends, late night (UTC)
- **Use gas trackers:** etherscan.io/gastracker
- **Transaction batching:** Combine multiple sends
- **Replace-by-Fee (RBF):** Speed up stuck transactions

Real-World Application: Exchange Withdrawal

What actually happens when you withdraw from Coinbase?

1. You request withdrawal to your wallet address
2. Exchange verifies your identity/2FA
3. Exchange creates transaction from *their* wallet
4. Exchange signs with *their* private key
5. Transaction enters mempool
6. Included in block (1 confirmation)
7. More blocks added (6 confirmations for Bitcoin)
8. Your wallet shows the balance

Key Insight

During this entire process, **you never touched the blockchain**.
You asked the exchange to make a transaction on your behalf.
This is why you don't control custodial funds – you're asking permission.

Application: Personal Security Checklist

Before using any cryptocurrency wallet:

Setup Phase

- ☐ Generated seed phrase offline?
- ☐ Written on paper (not digital)?
- ☐ Stored in secure location?
- ☐ Made backup copy?
- ☐ Tested recovery process?

Daily Use

- ☐ Verify addresses before sending
- ☐ Start with small test transaction
- ☐ Check network before confirming
- ☐ Review contract permissions

Red Flags to Avoid

- × Anyone asking for seed phrase
- × "Support" DMs on social media
- × Websites asking to "verify" wallet
- × Free token airdrops (often scams)
- × Urgent "limited time" offers

Best Practices

- ✓ Use hardware wallet for large amounts
- ✓ Enable all security features
- ✓ Keep software updated
- ✓ Never share private keys

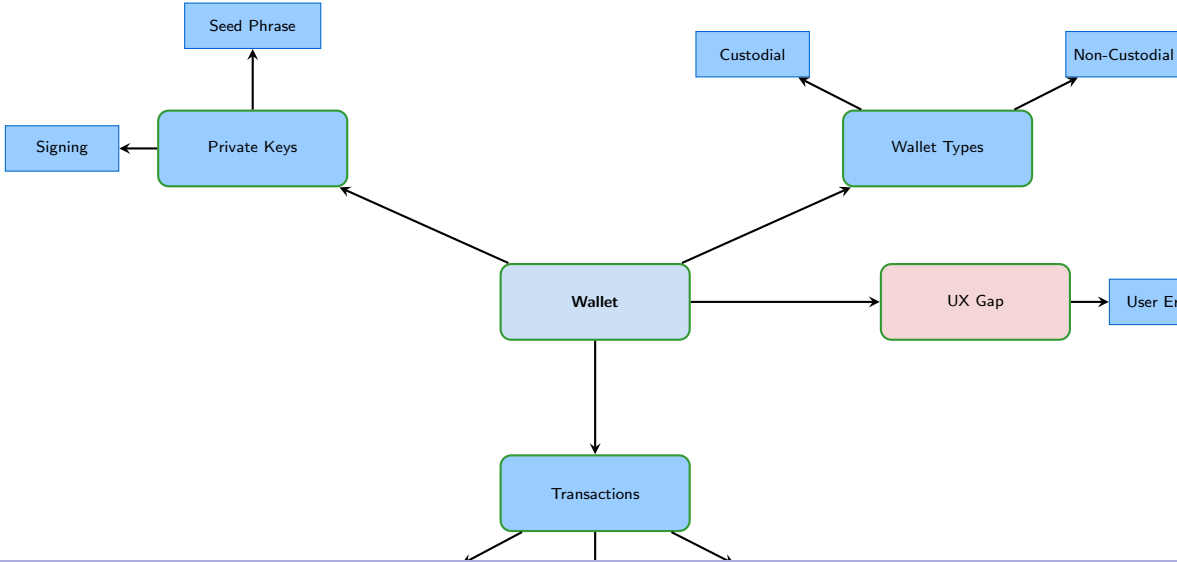
Executive Summary

Key Takeaways from Topic 3.3

1. **Wallets don't store crypto** – they store private keys that prove you can spend funds recorded on the blockchain.
2. **Wallet choice is a security/convenience tradeoff** – custodial wallets are easy but risky; self-custody is secure but demanding.
3. **"Not your keys, not your coins"** – if someone else holds your keys (exchanges), they control your funds.
4. **Transactions require gas** – fees are calculated as gas units $\times$ gas price, and fluctuate with network demand.
5. **The UX gap is real** – crypto demands users be their own bank, but most people aren't ready for that responsibility.

Bottom Line: Understanding wallets and transactions is essential for safely participating in the blockchain ecosystem.

Concept Map: The Wallet Ecosystem



Key Terms & Definitions (1/2)

Wallet A software or hardware tool that stores private keys and enables signing and broadcasting transactions.

Custodial Wallet A wallet where a third party (e.g., exchange) controls the private keys on the user's behalf.

Non-Custodial Wallet A wallet where only the user controls the private keys (self-custody).

Hot Wallet A wallet connected to the internet, convenient but more vulnerable to attacks.

Cold Wallet A wallet that stores keys offline, more secure but less convenient for frequent transactions.

Key Terms & Definitions (2/2)

Seed Phrase	A 12-24 word recovery phrase (BIP-39) that can regenerate all private keys in a wallet.
Gas	A unit measuring computational work on Ethereum; each operation costs a specific amount of gas.
Gwei	A denomination of ETH (10^{-9} ETH) commonly used to express gas prices.
Mempool	The "waiting room" where valid but unconfirmed transactions wait before being included in a block.
Confirmation	Each new block added after the block containing your transaction; more confirmations = more security.
UTXO	Unspent Transaction Output – Bitcoin's model for tracking ownership of coins.

Common Misconceptions

Myth vs. Reality

1. **Myth:** "My wallet stores my cryptocurrency."
   Reality: Your wallet stores *private keys*. The cryptocurrency exists as records on the blockchain.

2. **Myth:** "If I lose my password, the exchange can help me recover my funds."
   Reality: True for custodial wallets (exchange holds keys). False for non-custodial wallets – lose your seed phrase, lose everything.

3. **Myth:** "Blockchain transactions can be reversed if there's fraud."
   Reality: Blockchain transactions are *irreversible by design*. There's no "chargeback" like credit cards.

4. **Myth:** "Hardware wallets are unhackable."
   Reality: Hardware wallets significantly reduce risk but aren't perfect. Physical theft, supply chain attacks, and user error can still lead to loss.

Self-Assessment Questions (1/2)

Question 1: In Bitcoin's UTXO model, what happens when Alice wants to send 0.3 BTC but only has a single UTXO of 0.5 BTC?

A. The transaction is rejected because the amounts don't match exactly

B. She creates a transaction with the 0.5 BTC UTXO as input, 0.3 BTC to the recipient, and 0.2 BTC back to herself as change

C. The blockchain automatically splits the UTXO into smaller pieces before sending

D. The remaining 0.2 BTC is automatically sent to miners as a fee

Self-Assessment Questions (1/2)

Question 1: In Bitcoin's UTXO model, what happens when Alice wants to send 0.3 BTC but only has a single UTXO of 0.5 BTC?

A. The transaction is rejected because the amounts don't match exactly

B. She creates a transaction with the 0.5 BTC UTXO as input, 0.3 BTC to the recipient, and 0.2 BTC back to herself as change

C. The blockchain automatically splits the UTXO into smaller pieces before sending

D. The remaining 0.2 BTC is automatically sent to miners as a fee

Answer: B

In the UTXO model, transaction inputs must consume entire UTXOs. Alice must spend the full 0.5 BTC and explicitly create a "change" output returning 0.2 BTC to herself.

Self-Assessment Questions (2/2)

Question 2: What is the mempool in blockchain networks?

A. A secure storage location for private keys
B. A waiting area where unconfirmed transactions are held before being included in a block
C. A permanent archive of all historical transactions
D. A pool of rewards distributed to miners

Self-Assessment Questions (2/2)

Question 2: What is the mempool in blockchain networks?

A. A secure storage location for private keys
B. A waiting area where unconfirmed transactions are held before being included in a block
C. A permanent archive of all historical transactions
D. A pool of rewards distributed to miners

Answer: B – *The mempool is where valid but unconfirmed transactions wait.*

Question 3: What factors determine the size (and thus cost) of a blockchain transaction?

A. The transaction amount and the recipient's location
B. The number of inputs, outputs, and additional data (like smart contract calls)
C. The time of day and network traffic only
D. The cryptocurrency price and market volatility

Self-Assessment Questions (2/2)

Question 2: What is the mempool in blockchain networks?

A. A secure storage location for private keys
B. A waiting area where unconfirmed transactions are held before being included in a block
C. A permanent archive of all historical transactions
D. A pool of rewards distributed to miners

Answer: B – *The mempool is where valid but unconfirmed transactions wait.*

Question 3: What factors determine the size (and thus cost) of a blockchain transaction?

A. The transaction amount and the recipient's location
B. The number of inputs, outputs, and additional data (like smart contract calls)
C. The time of day and network traffic only
D. The cryptocurrency price and market volatility

Answer: B – *Transaction size depends on its data structure, not the amount sent.*

What's Next: Topic 3.4 – Bitcoin vs. Ethereum

Preview of the next topic:

Bitcoin

- "Digital Gold" philosophy
- Store of value focus
- UTXO model (as we learned)
- Limited scripting
- Conservative development

Ethereum

- "World Computer" vision
- Smart contract platform
- Account model
- Turing-complete programming (see Topic 3.4 for full explanation)
- Rapid innovation

Key Questions We'll Explore:

- Why do these two blockchains have such different designs?
- What are the tradeoffs of each approach?
- When would you use Bitcoin vs. Ethereum?

Topic 3.4 builds directly on the wallet and transaction concepts from today

Resources for Further Learning

Official Documentation

- Ethereum.org: "What is a wallet?" – ethereum.org/wallets
- Bitcoin Wiki: Transaction – en.bitcoin.it/wiki/Transaction
- EIP-1559 Explained – eips.ethereum.org/EIPS/eip-1559

Tools

- Etherscan Gas Tracker – etherscan.io/gastracker
- BTC Mempool Visualizer – mempool.space
- Transaction Simulator – tenderly.co

Books & Articles

- Antonopoulos, "Mastering Bitcoin" – Chapters 5-6 on Transactions
- Antonopoulos & Wood, "Mastering Ethereum" – Chapter 6 on Transactions
- Chainalysis 2023 Crypto Crime Report

Course Materials

- NB07: Blockchain Transaction Analysis (Jupyter notebook)

Questions?

Topic 3.3: Wallets, Transactions & The UX Gap

"Not your keys, not your coins."

Next: Topic 3.4 – Bitcoin vs. Ethereum