# Lab Session: Block Explorer Analysis

## BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

# Learning Objectives

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

- Navigate Etherscan and Blockstream block explorers effectively
- Analyze transaction details: inputs, outputs, fees, confirmations
- Trace transaction lifecycle from broadcast to confirmation
- Examine block structure and miner information
- Investigate address activity, balances, and transaction history
- Identify transaction patterns and entity types
- Conduct basic blockchain forensic analysis

# Lab Overview

**Structure:**

1. Introduction to block explorers (10 minutes)
2. Exercise 1: Analyzing Bitcoin transactions (20 minutes)
3. Exercise 2: Examining Ethereum transactions (20 minutes)
4. Exercise 3: Block analysis and mining (15 minutes)
5. Exercise 4: Address investigation (15 minutes)
6. Exercise 5: Forensic case study (20 minutes)
7. Wrap-up and deliverables (10 minutes)

**Total Duration:** 110 minutes

**Prerequisites:**

- Understanding of transaction structure (Lesson 6)
- Basic knowledge of Bitcoin and Ethereum
- Web browser with internet access

# What is a Block Explorer?

**Definition:**

- Web-based interface to query blockchain data
- Provides human-readable view of blocks, transactions, addresses
- Operates by indexing blockchain data (runs full node + database)
- Free and publicly accessible

**Major Block Explorers:**

**Bitcoin:**

- Blockstream.info (used by Blockstream, privacy-focused)
- Blockchain.com (oldest, most popular)
- Mempool.space (real-time mempool visualization)

**Ethereum:**

- Etherscan.io (most comprehensive, contract verification)
- Blockscout.com (open-source alternative)
- Ethplorer.io (token-focused)

**Key Features:**

- Search by transaction hash, block number, address
- View transaction status and confirmations
- Examine smart contract code and interactions
- Track token transfers (ERC-20, ERC-721)

# Exercise 1: Analyzing a Bitcoin Transaction

**Objective:** Understand Bitcoin UTXO model through real transaction

**Instructions:**

1. Visit: `https://blockstream.info`
2. Search for transaction hash:
   `f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16`
   (This is the first-ever Bitcoin transaction between Satoshi and Hal Finney, 2009)
3. Examine transaction details and answer:
   - How many inputs and outputs?
   - What is the total amount transferred?
   - What is the transaction fee?
   - Which block included this transaction?
   - How many confirmations does it have now?
4. Click on input address:
   - Observe sender's previous transactions
   - How was the UTXO created?
5. Click on output address:
   - Was this output spent or unspent?
   - If spent, in which transaction?

# Exercise 1: Key Observations

**Transaction Structure:**

- **Inputs:** Reference to previous transaction output (txid + index)
- **Outputs:** New UTXOs with amounts and recipient addresses
- **Fee:** Difference between input sum and output sum

**Understanding Confirmations:**

- Confirmations = number of blocks built on top of this transaction's block
- More confirmations = higher confidence transaction is final
- Historic transactions: 800,000+ confirmations
- Recent transactions: 1-10 confirmations

**UTXO Tracing:**

- Follow the chain of transactions backward (where did funds come from?)
- Follow forward (where did funds go?)
- Useful for: auditing, forensics, privacy analysis

**Questions to Consider:**

- Why do some transactions have many inputs or outputs?
- How can you identify change addresses?
- What does a very high fee indicate?

# Exercise 2: Analyzing an Ethereum Transaction

**Objective:** Understand Ethereum account model and gas fees

**Instructions:**

1. Visit: `https://etherscan.io`
2. Search for a recent transaction (click "Latest Transactions" on homepage)
3. Select a transaction and examine:
   - Transaction hash
   - Status (Success / Failed)
   - Block number
   - Timestamp
   - From address (sender)
   - To address (recipient or contract)
   - Value transferred (ETH amount)
   - Gas used vs. gas limit
   - Gas price and total transaction fee
4. If transaction involves smart contract:
   - Click "Logs" tab to see emitted events
   - Identify function called (e.g., "transfer" for ERC-20)
   - Observe internal transactions (contract calls)
5. Click on sender address:
   - View ETH balance
   - Examine transaction history
   - Check token holdings (ERC-20, NFTs)

# Exercise 2: Gas Mechanics

**Understanding Gas:**

- **Gas Limit:** Maximum gas user willing to pay
- **Gas Used:** Actual gas consumed by transaction
- **Gas Price:** Price per unit of gas (in gwei, 1 gwei $= 10^{-9}$ ETH)
- **Transaction Fee:** Gas Used $\times$ Gas Price

**Post-EIP-1559 (August 2021):**

- **Base Fee:** Algorithmically determined, burned
- **Priority Fee (Tip):** Paid to miner/validator
- **Max Fee:** Maximum total fee user willing to pay

**Example Calculation:**

- Gas Used: 21,000 (simple ETH transfer)
- Base Fee: 30 gwei
- Priority Fee: 2 gwei
- Total Fee: $21,000 \times (30 + 2) = 672,000$ gwei $= 0.000672$ ETH
- At ETH $=$ \$2,000: fee $=$ \$1.34

**Failed Transactions:**

- Gas still consumed (computation executed)
- State changes reverted
- Common causes: out of gas, failed assertion, contract error

# Exercise 3: Block Analysis

**Objective:** Understand block structure and mining/validation

**Bitcoin Block Analysis:**

1. On Blockstream.info, search for block 800,000 (milestone block)
2. Examine block header:
   - Block hash
   - Previous block hash (forms chain)
   - Merkle root (commitment to all transactions)
   - Timestamp
   - Difficulty and nonce (proof-of-work)
3. Identify coinbase transaction (first transaction):
   - Block reward amount (6.25 BTC as of 2024)
   - Transaction fees collected
   - Miner address (who mined this block?)
4. Count transactions in block
5. Calculate average transaction fee

**Ethereum Block Analysis:**

1. On Etherscan.io, view latest block
2. Examine block details:
   - Validator (who proposed block?)
   - Gas used / gas limit
   - Base fee per gas
   - Burnt fees (EIP-1559)

# Exercise 4: Address Investigation

**Objective:** Analyze address activity and identify entity types

**Instructions:**

1. **Exchange Address (Example: Binance Hot Wallet)**
   - Search Etherscan for: `0x28C6c06298d514Db089934071355E5743bf21d60`
   - Observe transaction volume (thousands per day)
   - Note large balances (millions of USD)
   - Identify patterns: frequent deposits and withdrawals
   - Tag: Etherscan labels it "Binance 14"
2. **Smart Contract Address**
   - Search for Uniswap V3 Router: `0xE592427A0AEce92De3Edee1F18E0157C05861564`
   - Click "Contract" tab to view verified source code
   - Examine recent transactions (all contract interactions)
   - Notice: no ETH balance needed (users pay gas)
3. **Individual User Address**
   - Use your own MetaMask address (from Lab 8)
   - View transaction history
   - Check token balances
   - Compare activity level with exchange address

# Exercise 4: Entity Identification Patterns

**How to Identify Address Types:**

**Exchange Addresses:**
- Very high transaction volume (1000s per day)
- Large balances (millions of USD)
- Many unique counterparties
- Often labeled by block explorers
- Pattern: users deposit -¿ internal accounting -¿ users withdraw

**Smart Contracts:**
- "Contract" label in block explorer
- Transactions show "Contract Interaction"
- Code visible (if verified)
- Receives transactions, never initiates (unless self-destruct)

**Individual Users:**
- Low-to-moderate transaction volume
- Smaller balances
- Irregular transaction timing
- Mix of incoming and outgoing transactions

**Miners/Validators:**
- Receive coinbase rewards (Bitcoin)

# Exercise 5: Forensic Case Study

**Scenario: Tracking Stolen Funds**

Imagine you are a blockchain analyst investigating a theft. Your task is to trace the flow of stolen funds.

**Case Details:**

- Victim address (hypothetical): `0xVICTIM`
- Attacker address (hypothetical): `0xATTACKER`
- Transaction hash of theft: `0xSTEAL`
- Amount stolen: 100 ETH

**Investigation Steps:**

1. **Confirm Theft:**
   - Search for transaction `0xSTEAL`
   - Verify 100 ETH moved from victim to attacker
2. **Trace Funds:**
   - Click on attacker address
   - View subsequent transactions
   - Identify where 100 ETH went (direct transfer? split? mixer?)
3. **Follow the Chain:**
   - If funds moved to another address, continue tracing
   - If funds sent to exchange, investigation pauses (off-chain)
   - If funds sent to mixer/tumbler, tracing becomes difficult
4. **Document Path:**
   - Create flowchart: Victim -¿ Attacker -¿ Address A -¿ Address B -¿ Exchange
   - Note transaction hashes at each step

# Exercise 5: Privacy and Mixing

**Blockchain Privacy Challenges:**

- All transactions publicly visible
- Addresses pseudonymous but traceable
- Address reuse links multiple transactions to same entity
- Heuristics identify common ownership (e.g., inputs from same transaction)

**Privacy Techniques:**

1. **Mixers/Tumblers (e.g., Tornado Cash):**
   - Pool funds from many users
   - Withdraw to new address
   - Breaks on-chain link
   - Controversial: used by criminals but also privacy advocates
2. **CoinJoin (Bitcoin):**
   - Multiple users combine transactions
   - Obfuscates sender-receiver mapping
   - Used by Wasabi Wallet, Samourai Wallet
3. **Privacy Coins (Monero, Zcash):**
   - Built-in privacy (ring signatures, zero-knowledge proofs)
   - Transactions not traceable
   - Trade-off: regulatory scrutiny, exchange delistings

**Ethical Considerations:**

- Privacy as a right vs. transparency for accountability
- Law enforcement vs. individual freedom

# Advanced Block Explorer Features

**Etherscan Tools:**

1. **Contract Verification:**
   - Developers upload source code
   - Etherscan compiles and matches bytecode
   - Users can read contract logic before interacting
2. **Token Tracker:**
   - View all ERC-20 tokens
   - See total supply, holders, transfers
   - Identify top holders
3. **Gas Tracker:**
   - Real-time gas price recommendations
   - Historical gas price charts
   - Gas usage by contract (which dApps are expensive?)
4. **Charts and Analytics:**
   - Daily transaction count
   - Network utilization
   - ETH supply and burn rate
   - Validator statistics

**Mempool Explorers:**

- Mempool.space (Bitcoin): visualize pending transactions
- See fee distribution, block template predictions
- Useful for fee estimation

# Lab Deliverables

**Submit the following:**

1. **Transaction Analysis Report (2-3 pages PDF):**
   - Exercise 1: Bitcoin transaction hash, input/output summary, fee analysis
   - Exercise 2: Ethereum transaction hash, gas breakdown, sender/recipient details
   - Exercise 3: Block number analyzed, coinbase/validator info, statistics
   - Exercise 4: Three addresses investigated with entity type identification
   - Exercise 5: Forensic case flowchart (real or hypothetical scenario)
2. **Screenshots:**
   - Bitcoin transaction details page
   - Ethereum transaction details page
   - Block details page
   - Address activity page
   - (Annotate screenshots with key observations)
3. **Reflection Questions (1 page):**
   - How does blockchain transparency affect privacy?
   - What are legitimate uses of transaction mixers?
   - How can forensic analysis help recover stolen funds?
   - What limitations exist in blockchain forensics?
4. **Bonus (Optional):**
   - Analyze the same address on Bitcoin and Ethereum (if applicable)
   - Investigate a recent high-profile hack using block explorer

# Key Takeaways

- Block explorers provide transparency into all blockchain activity
- Bitcoin uses UTXO model: trace inputs and outputs
- Ethereum uses account model: track balances and nonces
- Gas fees vary based on network congestion and transaction complexity
- Addresses can be identified by transaction patterns (exchanges, contracts, users)
- Blockchain forensics is powerful but faces challenges with mixers and privacy coins
- Verified smart contracts allow users to audit code before interacting
- Mempool analysis helps estimate fees and transaction timing

**Real-World Applications:**

- Auditing and compliance
- Fraud investigation and fund recovery
- Market analysis (whale watching, exchange flows)
- Security research (identifying attack patterns)

# Discussion Questions

1. How does Bitcoin's UTXO model differ from Ethereum's account model in terms of privacy?
2. Why are transaction fees so variable on Ethereum compared to Bitcoin?
3. What are the ethical implications of blockchain transparency?
4. How can someone enhance their privacy when using public blockchains?
5. What role do block explorers play in blockchain adoption?
6. How might regulation affect block explorer operations in the future?

# Module A Summary and Next Steps

**What You Learned in Module A:**

- Blockchain fundamentals: decentralization, immutability, transparency
- Distributed ledger technology and consensus mechanisms
- Hash functions and cryptographic security
- Public key cryptography and digital signatures
- Bitcoin protocol: UTXO model, transactions, scripting
- Proof-of-work and proof-of-stake consensus
- Consensus mechanism trade-offs and comparisons
- Scalability trilemma and Layer 2 solutions
- Practical skills: wallet setup, transaction analysis, block exploration

**Preparation for Module B (Smart Contracts and DeFi):**

- Review Ethereum fundamentals
- Explore DeFi applications (Uniswap, Aave, Compound)
- Familiarize yourself with Solidity programming concepts
- Keep MetaMask wallet active with testnet ETH