Blockchain Investigation Visual Reference

A comprehensive guide for cryptocurrency forensic analysis and investigation

1 Blockchain Basics

Key Concepts

- Block: Collection of transactions confirmed together
- Transaction: Transfer of value between addresses
- Address: Public identifier for sending/receiving
- Private Key: Secret that controls address funds
- Hash: Unique fingerprint of data

Verification Mechanisms

- Proof of Work: Resource-intensive puzzle solving
- Proof of Stake: Validators stake crypto as collateral
- Delegated PoS: Elected validators by token holders

2 Address Formats

Bitcoin

- `1...` - P2PKH (Legacy)
- `3...` - P2SH (Segwit)
- `bc1...` - Bech32 (Native Segwit)

Ethereum

- `0x...` - Standard format (42 chars)
- Contracts use same format as EOAs

Other Formats

- `T...` - TRON
- `ltc1...` - Litecoin (Bech32)
- `bnb...` - Binance Chain

Privacy Coins

- `4...` - Monero (Standard)
- `8...` - Monero (Subaddress)
- `z...` - Zcash (Shielded)

```
Example BTC: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Example ETH: 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045
```

3 Blockchain Types

Public Blockchains

- Bitcoin (BTC)
- Ethereum (ETH)
- Litecoin (LTC)
- BNB Chain (BNB)

Privacy-Focused

- Monero (XMR)
- Zcash (ZEC)
- Dash (DASH)
- Grin (GRIN)

Investigation Difficulty Scale

Easy: Bitcoin, Litecoin - Clear UTXO model
Moderate: Ethereum - Smart contracts add complexity
Hard: ZCash (transparent tx only)
Very Difficult: Monero, ZCash (shielded tx)

Transparency Features

Public Ledger: All transactions visible
Pseudo-anonymity: Addresses not linked to identity
Immutable History: Cannot alter past records

4 Transaction Anatomy

UTXO Model (BTC)

- Inputs: Previous UTXOs being spent
- Outputs: New UTXOs being created
- Change: Returned to sender
- Fee: (Inputs - Outputs)

Account Model (ETH)

- From: Sender address
- To: Recipient address
- Value: Amount transferred
- Gas: Fee paid for execution

Transaction Properties

Property	Bitcoin	Ethereum
Confirmations	~6 blocks (60 min)	~12 blocks (3 min)
Fee Structure	Satoshis/byte	Gas × Gas Price
Finality	Probabilistic	Probabilistic
Transaction ID	Double SHA-256 hash	Keccak-256 hash

5 Address Clustering Techniques

Co-spend Heuristic

Addresses used as inputs in the same transaction are controlled by the same entity.

Change Address Detection

Techniques to identify outputs that return to the sender:

- Address reuse pattern: Previously used as change
- Output value analysis: Odd amounts likely change
- Script type: Different from spending address
- Behavior analysis: Used shortly after as input

Caution: Change detection is probabilistic, not deterministic. Always evaluate multiple factors before making conclusions.

Multi-Input Transactions

When a wallet needs to spend more than one UTXO to cover a payment amount, it creates a transaction with multiple inputs, revealing address connections.

Behavioral Patterns

Regular transaction timing (e.g., weekly withdrawals), consistent amount patterns, or repeated interaction with specific services indicates shared control.

Deterministic Wallets

HD wallets generate addresses from a single seed. Some services use predictable derivation patterns that can be identified through analysis.

6 Investigation Tools

Blockchain Explorers

- Blockchair: Multi-blockchain explorer
- Blockchain.com: Bitcoin, ETH, BCH explorer
- Etherscan: Ethereum-focused explorer
- BscScan: BNB Chain explorer
- TxStreet: Visual mempool representation

Commercial Platforms

- Chainalysis: Enterprise-grade analysis
- CipherTrace: AML & compliance tools
- Elliptic: Risk management platform
- Crystal Blockchain: Analytics suite
- TRM Labs: Risk management & analytics

Open-Source Tools

- BlockSci: Python blockchain analysis framework
- GraphSense: Crypto analytics platform
- Bitcoin Explorer (bx): Command-line tools
- Maltego: Graph-based investigation
- Bitlodine: BTC clustering/tagging

API Services

- OKLink: Multi-chain data
- BlockCypher: Transaction propagation
- Amberdata: Historical blockchain data
- Alchemy: Enhanced Ethereum data
- Tokenview: Automated analytics

Tool Comparison Matrix

Tool	Best For	Chains	Price	Visualization
Chainalysis	Enterprise/Gov	20+	$$$$$	Advanced
OKLink	Multi-chain	15+	$$$	Good
BlockSci	Research	UTXO only	Free	Custom
GraphSense	Clustering	5+	Free	Good

7 Transaction Flow Analysis

Taint Analysis

Taint analysis traces how funds from a specific source (e.g., stolen coins) flow to destination addresses.

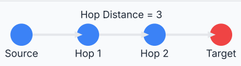
Forward Taint: Tracks where funds went after leaving a flagged address.

Backward Taint: Traces the origin of funds that arrived at a specific address.

Taint Calculation Methods

- Poison: One tainted input taints all outputs
- Haircut: Proportional taint distribution
- FIFO/LIFO: Time-ordered coin spending

Hop Analysis



Hop Distance Characteristics

- 1-2 hops: Direct connections, high confidence
- 3-5 hops: Moderate distance, potential relation
- 6+ hops: Distant connection, weak relationship

Note: Mixers, exchanges, and mining pools act as "hop barriers" that make connections less conclusive. Treat transactions through these entities with caution.

Temporal Analysis

Time Patterns

- Transaction time clustering
- Regular interval detection
- Time zone analysis

Value Patterns

- Round number transactions
- Consistent percentage splits
- Fee anomaly detection

Behavioral Indicators

- Peeling chains (sequential txs)
- Fan-out/fan-in patterns
- Dormancy periods

8 Suspicious Transaction Patterns

Money Laundering Indicators

- Layering: Multiple rapid transfers between addresses
- Structuring: Breaking large amounts into smaller ones
- Round-trip transactions: Funds returning to origin
- Exchange hopping: Moving across multiple exchanges
- Mixer usage: Passing through anonymizing services

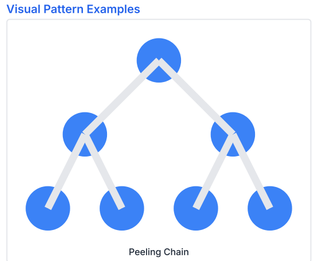
Red Flags: Rapid succession transactions, unused outputs, dormant address activation, chain hopping (BTC→XMR→ETH)

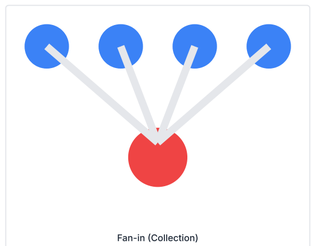
Common Scam Patterns

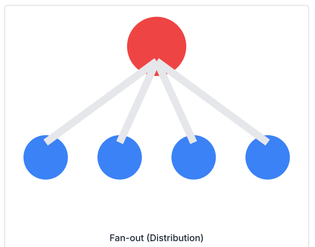
- Giveaway scams: Small deposits, no withdrawals
- Ponzi schemes: Pyramid distribution pattern
- Fake ICOs: Large collection, rapid distribution
- Rug pulls: Dev wallets emptying liquidity pools
- Phishing: Immediate outflow after deposit

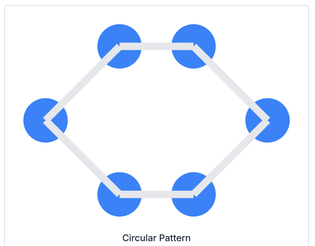
Note: Legitimate entities like exchanges may also display some of these patterns. Always corroborate with additional evidence and entity identification.

Visual Pattern Examples


Peeling Chain


Fan-in (Collection)


Fan-out (Distribution)


Circular Pattern

Ransomware Indicators

- Multiple identical ransom payments to same address
- Specific requested amount (e.g., 0.3 BTC exactly)
- Payments consolidated then moved to exchanges
- Temporal correlation with reported attacks

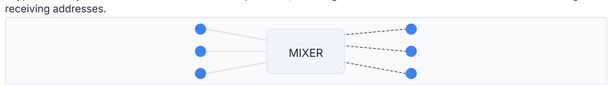
Darknet Market Indicators

- High volume of small deposits to single address
- Scheduled batch withdrawals (vendor payouts)
- Escrow address usage patterns
- Multisig transaction structures

9 Mixers & Tumblers

How They Work

Cryptocurrency mixers combine funds from multiple users, shuffling them to break transaction trails between sending and receiving addresses.



Detection Features

- Time delay patterns: Standard wait times
- Fee structures: Fixed % or tiered fees
- Amount standardization: Fixed denominations
- Address reuse: Temporary collection addresses

Known Mixer Services

- Wasabi Wallet (CoinJoin)
- Samourai (Whirlpool)
- Tornado Cash (ETH)
- ChipMixer (BTC)

Note: Many jurisdictions consider mixer usage suspicious. Some services (Tornado Cash) have been sanctioned by regulators.

10 Entity Identification

Exchange Fingerprinting

- Deposit addresses: Known patterns & prefixes
- Withdrawal patterns: Timing, amounts, batching
- Hot/cold wallet transfers: Security patterns
- Fee structures: Unique to each platform

Common Entity Tags

Exchange | Mining Pool | Mixer | Merchant | Darknet | Payment Processor | Gambling | DeFi Protocol

Entity Identification Methods

- Known address lists: Public entity disclosures
- Network analysis: Transaction patterns
- Off-chain intelligence: Forum posts, social media
- Self-attributions: Signed messages, website info

Risk Scoring

Low (1-3): Regulated exchanges, known entities
Medium (4-7): Unregulated services, gambling
High (8-10): Mixers, darknet markets, ransomware

Factors: Entity type, jurisdiction, KYC practices, regulatory compliance

11 Forensic Data Sources

Blockchain Data

- Transaction history: All on-chain movements
- Block data: Timestamps, miner info
- Mempool: Pending transactions
- Smart contract code: On-chain logic

External Data Sources

- Exchange records: KYC, trading history
- Forum disclosures: Self-identified addresses
- Darknet marketplaces: Seized server data
- IP association: Transaction broadcast data
- Social media: Address sharing, scam reports

Data Collection Methods

- Full node operation: Direct blockchain access
- API services: Preprocessed blockchain data
- OSINT techniques: Public information gathering
- Subpoenas: Legal requests to service providers

Data Challenges

- Chain-hopping obscures complete flow
- Off-chain transactions (Lightning Network)
- Privacy protocols (Monero, zkSNARKs)
- Exchange pooled wallets lack attribution

12 Case Study Framework

Investigation Elements

- Initial indicators: Suspicious activity triggers
- Source of funds: Origin identification
- Flow analysis: Transaction path mapping
- Entity attribution: Wallet owner identification
- Value calculation: Monetary impact assessment
- Evidence chain: Forensically sound documentation

Documentation Structure

Case Summary

- Case identifier
- Date range
- Entities involved
- Value at risk
- Methodology

Key Findings

- Address clusters
- Entity attributions
- Transaction patterns
- Risk indicators
- Timeline

Famous Cases

Case	Year	Value	Resolution
Silk Road	2013	175,000 BTC	Seized
Mt. Gox	2014	850,000 BTC	Partial recovery
Bitfinex Hack	2016	119,754 BTC	Partial recovery
Colonial Pipeline	2021	75 BTC	Partial recovery

13 Learning Resources

Books & Publications

- Investigating Cryptocurrencies - Nick Furneaux
- Bitcoin Forensics - James Harris
- Cryptoasset Inheritance Planning - Pamela Morgan
- The Basics of Bitcoins and Blockchains - Antony Lewis
- CryptoAssets - Chris Burniske & Jack Tatar

Courses & Certifications

- Certified Cryptocurrency Investigator (CCI) - CipherTrace
- Cryptocurrency Tracing - Chainalysis
- Certified Blockchain Expert - Blockchain Council
- Cryptocurrency Investigation - ACAMS
- Financial Crime Academy - Elliptic

Online Resources

- Cambridge Cryptoasset Study - Cambridge University
- CryptoCompare Research - Market insights
- Crystal Blockchain Blog - Analytics insights
- Chainalysis Market Intel - Market reports
- FATF Guidelines - Regulatory resources
- ACFCS Articles - Case studies

Recommended Learning Path

Blockchain Basics → Transaction Analysis → Clustering Techniques → Pattern Recognition → Case Building

Tools Mastery Path

1. Learn public block explorers (Blockchair, Etherscan)
2. Practice with open-source analysis tools (BlockSci)
3. Develop visualization skills (Gephi, Maltego)
4. Build automation skills (Python for blockchain)
5. Adopt professional platforms when needed

Practice Resources

- CryptoHack - Cryptography challenges
- Follow The Coin - Transaction tracing game
- BlockSec CTF - Security competitions
- Princeton Bitcoin Course - Online lectures
- GitHub repositories - Open-source tools

14 Chain Hopping Techniques

What is Chain Hopping?

Chain hopping is the practice of moving assets between different blockchains to obscure the trail of funds and take advantage of the different privacy characteristics of each network.

Investigation Challenges

- Cross-chain tracing: Service attribution required
- Data silos: Different explorers for each chain
- Privacy barriers: Some chains obscure information
- Timing correlation: Matching deposits/withdrawals
- Exchanges as black boxes: Internal transfers hidden

Blind Spots: When funds move through privacy chains like Monero or through mixers/tumblers, the trail often goes cold.

Common Hopping Patterns

Privacy Seeking
BTC → XMR → ETH → BTC
Purpose: Break transaction trail
Detection: Timing correlation of exchange deposits/withdrawals

Fee Optimization
BTC → LTC → Exchange → BTC
Purpose: Lower transaction fees
Detection: Consistent amount minus predictable fees

Regulatory Evasion
Regulated → Unregulated Exchange → Privacy Coin
Purpose: Avoid reporting/restrictions
Detection: Exchange API identification, withdrawal patterns

Investigation Approaches

- Service Node Operation: Capturing network data
- Exchange Cooperation: Legal process access
- Deposit/Withdrawal Correlation: Timing analysis
- Amount Tracking: Distinct value patterns
- Known Exchange Patterns: Hot wallet signatures
- Integrated Services: Multi-chain analysis platforms

Best Practice: Focus on exchange chokepoints where funds enter and exit privacy layers. Most users eventually convert back to transparent chains.

15 Smart Contract Analysis

Key Contract Types

- ERC-20 Tokens: Fungible token standard
- ERC-721/1155: NFT standards
- DEX Contracts: Decentralized exchanges
- Lending Protocols: DeFi lending platforms
- DAO Governance: Voting contracts
- Multisig Wallets: Shared control contracts

Common Smart Contract Exploits

- Reentrancy: Recursive calling of vulnerable function
- Flash Loan Attacks: Temporary large-sum borrowing
- Oracle Manipulation: Price feed tampering
- Front-running: Transaction order manipulation

Analysis Techniques

- Event Logs: Transaction event tracking
- Internal Transactions: Contract-to-contract calls
- Method Signatures: Function identification
- State Changes: Variable modifications
- Token Flows: Transfers between addresses
- Contract Code: Behavior examination

```
// Ethereum Contract Call Analysis Example
contract.transfer(recipient, amount);
// Translates to function signature:
0xa9059cbb // transfer(address,uint256)
// Event emmitted (topic):
0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef // Transfer
```

Investigation Tools

Block Explorers

- Etherscan, BscScan, PolygonScan
- Blockscan (for multiple EVM chains)
- Tenderly (advanced debugging)

Analysis Platforms

- Dune Analytics (SQL queries)
- Nansen (wallet profiling)
- Etherscan Decompiler

Development Tools

- Remix IDE (code analysis)
- Hardhat (local testing)
- Slither (security scanner)

16 DeFi Investigation

DeFi Protocol Types

- DEXs: Uniswap, SushiSwap, PancakeSwap
- Lending: Aave, Compound, MakerDAO
- Yield Farming: Yearn, Curve, Convex
- Derivatives: dYdX, Synthetix, Perpetual
- Bridges: Wormhole, Multichain, Portal

Common DeFi Attacks

- Flash Loan Exploits: Large funds for single-tx attacks
- Economic Attacks: Pool value manipulation
- Governance Attacks: Token voting manipulation
- Bridge Exploits: Cross-chain validation flaws
- Rugpulls: Developer-controlled asset draining

Tracing DeFi Transactions

Token Swap → LP Position → Yield Farming → Bridge Transfer → New Chain

Investigation Challenges

- Multiple contract interactions per transaction
- Complex logic across multiple protocols
- Token swaps change asset identifiers
- Cross-chain movements break tracing

Investigation Techniques

- Track net value changes across interactions
- Follow internal transactions (contract-to-contract)
- Identify protocol signatures and events
- Monitor bridge endpoints on both chains

Specialized Tools

- DeBank (cross-chain portfolio tracking)
- Zerion (DeFi transaction history)
- DeFiLlama (protocol analytics)
- APY.Vision (liquidity pool analysis)