Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations

Pascal Tippe, Christoph Deckers

FernUniversität in Hagen

April 4, 2025

Bitcoin: Fundamentals for Investigations

Bitcoin Basics

- Decentralized cryptocurrency created in 2009
- Based on blockchain: public, transparent ledger of all transactions
- Every transaction permanently recorded and viewable by anyone
- Global peer-to-peer network without central authority

Transactions Structure

- Funds move between addresses (strings like 1A1zP1...)
- Addresses are linked to cryptographic key pairs, not identities
- Transactions require digital signatures from sending addresses
- Multiple inputs and outputs in single transactions

Bitcoin: Privacy Challenges

Pseudonymity vs. Anonymity

- Bitcoin is pseudonymous, not anonymous
- Addresses serve as persistent public identifiers
- Anyone can view complete transaction history of any address

Blockchain Analysis Capabilities

- Transaction patterns can link addresses to real-world identities
- Heuristics attempt to group addresses by ownership
- Simple transfers leave clear trails on the blockchain

Implications for Criminal Investigations

- Blockchain transparency creates powerful forensic opportunities
- Need for privacy drives development and use of mixing services

Bitcoin Mixers: Technical Overview

What Are Bitcoin Mixers?

- Services that *mix* transactions from multiple users to obscure fund origins
- Break the direct connection between sending and receiving addresses
- Also known as ”tumblers” or ”coin shufflers”

Mixer Typology

Centralized Mixers

- Third-party custodial services
- Proprietary mixing algorithms
- Service fees: 0.5-5% per transaction

Decentralized Mixers

- Protocol-based (i.e. CoinJoin)
- Non-custodial, smart contract-driven
- Multiple users pool transactions

Key Challenges in Mixer Investigations

- Breaking the deliberate obfuscation layer
- Dealing with:
    - Multiple transaction "hops"
    - Irregular time delays
    - Fragmented transaction amounts
- Heuristic limitations when mixing is properly executed
- Jurisdictional and legal complexities
- Balance between legitimate privacy and illicit use cases

Current Mixer Landscape: Market Analysis

- Surveyed cryptocurrency forums (Bitcointalk, Reddit)
- Identified 20 active mixing services

Key Findings

- No services required registration/KYC
- Only 1 service allowed multiple input addresses
- 17/20 supported multiple output addresses
- 10/20 offered customizable delay options
- Delays ranged from immediate to 168h

- 19/20 maintained clearnet domains
- 13/20 used Cloudflare to mask locations
- 19/20 operated Tor Onion Services
- 15/20 provided signed letters of guarantee
- 9 services: short delays ($\leq$8h)
- 8 services: long delays ($>$24h)

Bitcoin Mixer Prosecutions: Scale of Operations

Three Major U.S. Cases (2019-2023)

- Significant criminal prosecutions providing insights into mixer operations
- Cases represent varied scales and operational timeframes

Scale of Operations

- **ChipMixer (2023)**
  - Processed approximately $3 billion in cryptocurrency
  - Operated for more than 5 years
- **Helix (2019)**
  - Laundered over $300 million in Bitcoin
  - Operated for approximately 3 years
- **Bitcoin Fog (2021)**
  - Moved approximately 1.2 million Bitcoin (approximately $400 million)
  - Long-running mixer (operated 2011-2021)

Bitcoin Mixer Investigations: Key Findings

Critical Investigation Methods

- Law enforcement conducted test transactions in all cases
- However, test transactions *alone* did not identify operators

Investigation Breakthroughs

- **ChipMixer**: FBI identified IP address of Tor Onion Service
- **Bitcoin Fog**: Traced bitcoins used to pay for domain hosting
- **Helix**: Technical details not disclosed

Implications for Investigations

- Purely blockchain-based analysis has significant limitations
- Traditional investigative methods remain essential
- Technical infrastructure critical vulnerability

Methodology: Test Transactions & Graph Analysis

- Selected two operational Bitcoin mixing services for analysis
- Conducted controlled test transaction through each mixer
- Created property graph model in Neo4j database
- Graph queries to identify transaction patterns and relationships
- Visualization to reveal complex transaction flows and mixer behaviors

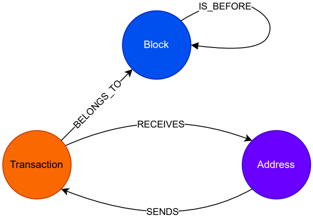
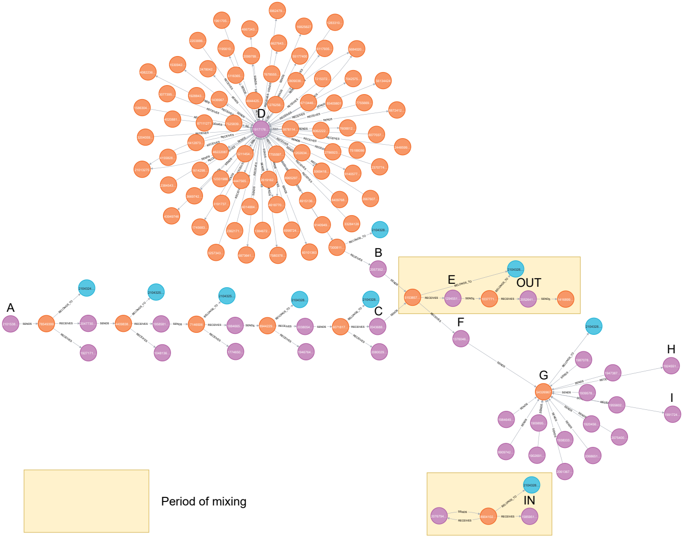


Figure: Neo4j visualization of Bitcoin transactions showing mixer patterns with address nodes (purple), transaction nodes (orange), blocks (blue) and their relationships

Transaction Analysis: Tracing the Mixers

- Checked for a path between input and output (direct linkage)
- Transaction value analysis
  - Analyze output address candidates within maximum mixing time delay
  - Search for suitable transaction values (input - fee)
- Further manual graph inspection for other indicators
  - Annotated relevant addresses with CrystalBlockchain and AMLBot
- **Mixer 1**
  - Maximum 1 output address, maximum 24 hours mixing delay
  - Couldn't validate signed letter of guarantee
- **Mixer 2**
  - Maximum 2 output addresses, maximum 24 hours mixing delay
  - Couldn't validate signed letter of guarantee
  - Claimed to source bitcoins for payout from cryptocurrency exchanges

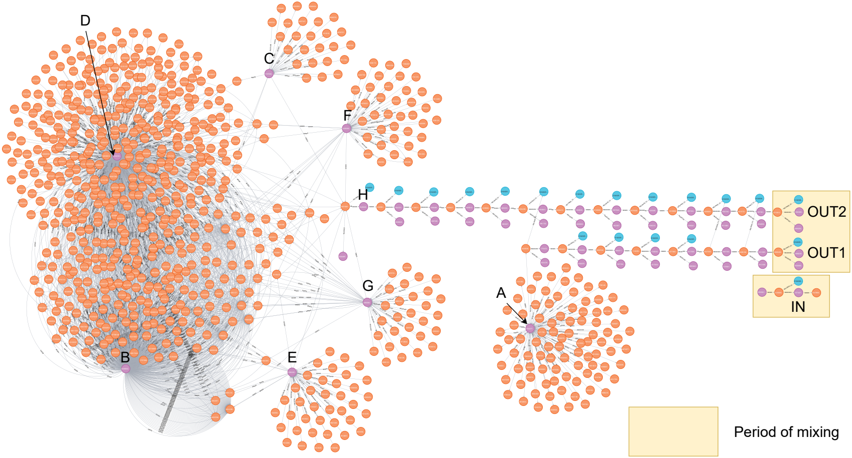
Bitcoin Mixer 1 Output Payment Analysis



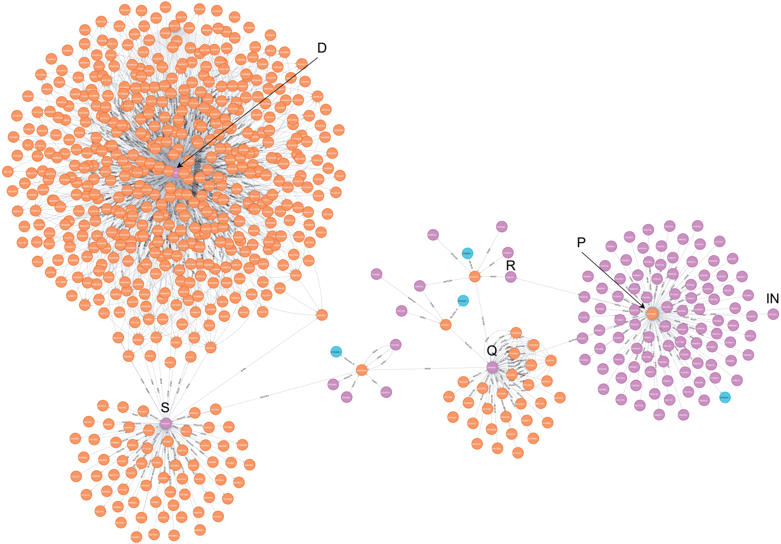
Bitcoin Mixer 1 Analysis

- No direct linkage between input and output
- Transaction value analysis with default fee returned only two candidate addresses
  - The entire fee range yields 4,453 candidate addresses
- Annotations show no blacklisted or suspicious addresses
- Output payment: Two transaction in one block!
- Input payment was not processed (even more than two months later)

Bitcoin Mixer 2 Output Payment Analysis



Bitcoin Mixer 2 Input Payment Analysis



Bitcoin Mixer 2 Analysis

- No direct (visual) linkage between input and output
  - Path in graph due to address reuse
- Transaction value analysis
  - Assuming a single payout address with entire fee range: 1,422 transactions
  - With two output addresses: 391,998 (every possible value between 0 and expected amount - fee)
  - Two output addresses mitigate this attack
- Annotations show two blacklisted and one suspicious address
  - Multiple addresses linked to HTX cryptocurrency exchange
  - Mixer likely uses these to pay mixing service users

Investigative Angles

- Striking characteristics for Mixer 1
- Transaction value analysis simple and (partially) effective
  - Multiple output addresses and long mixing delays mitigate this attack
  - Can also incorporate external knowledge: Mixing time, fee settings
- Quickly freeze cryptocurrency exchange accounts
  - If not identifying lead → Cause considerable economic damage
- 13 out of 20 mixing services use Cloudflare
  - Wiretap connections?