Cryptocurrency Transaction Investigation Guide

This guide provides a framework for investigating cryptocurrency transactions, offering practical steps and considerations for private investigators, law enforcement, and cybersecurity professionals. Due to the unique nature of cryptocurrencies, these investigations require specialized knowledge and techniques.

Understanding the Investigation

- **Key Questions:** The primary goal of a cryptocurrency investigation is often to trace the flow of funds. When following the money, it is important to consider if this a compliance issue or an actual investigation? Either way, this may involve identifying the source of funds, destination, and any intermediaries involved. The specific questions will vary based on the nature of the investigation (e.g., fraud, money laundering, sanctions evasion).
- **Types of Investigations:** Different investigations require different investigative methods. For example, an elderly person putting money into a Bitcoin ATM is not the same as a counter-terrorism investigation. There are many different investigation types which can include, but not limited to, ransomware, romance scams, darknet market transactions, theft, etc.).

Information Gathering

Gathering the right information is paramount in an investigation. The challenge is not all people understand what information the investigator requires and may not have that information readily available. Help the victim in gathering the necessary information.

- **Essential Data For An Investigation:**
  - Transaction hash
  - Blockchain (e.g., Bitcoin, Ethereum)
  - Token type (if applicable)
  - Date/time of transaction(s)
  - Sending and receiving addresses
  - Transaction receipts (if available)

While screenshots of transaction data is better than nothing, it greatly increases the chance of human error while transcribing said data. Therefore, it is highly recommended that transaction data be provided in spreadsheet format.

- **Supporting Evidence:**
  - Communication logs (WhatsApp, Telegram, emails, etc.)
  - Victim interviews: Include your points about building trust, active listening, and understanding the victim's emotional state.
  - Background information: How the victim encountered the scammer, the progression of the scam, the first and last transactions, and any ongoing communication.

High-Level Investigative Process

Initial Intake: Document the case details (who, what, where, when, why). Using a standardized intake form to collect preliminary information can be helpful in making sure the most important details are not lost or overlooked.

Victim Interview: Conduct a live interview (in-person or remote) to gather detailed information and build rapport with the victim. Build trust and actively listen, paying attention to body language and other nonverbal cues, such as signs of fear, nervousness, or defensiveness.

Set expectations at this stage, including, but not limited to,

- How are investigations conducted? Investigator's role, Law enforcement's involvement, Legal procedures involved.
- What to expect? – timelines (stages of investigation), overall chance of recovering tokens or funds.

This helps the victim understand what the process is and whether it is worth the cost and effort.

Blockchain Analysis: Use blockchain explorer tools and specialized software to trace transactions, identify addresses, and analyze patterns. Follow the flow of funds to identify the ultimate destination and potentially recover stolen assets.

Open Source Intelligence (OSINT): Leverage online resources to gather information about the transactions' addresses, individuals, or entities involved.

Law Enforcement Collaboration: (If applicable) Work with law enforcement agencies to obtain subpoenas, warrants, or other legal assistance.

Conducting The Investigation

Here are more detailed steps on how the actual investigative work is conducted. Keep in mind that **timing is very important in an investigation.**

Step 1: Using preliminary information, determine whether or not **this case is worth working on.** If possible, taking a quick look at transaction data with the use of forensic tools can be useful in determining if the money can be traced to cooperative entities.

Step 2: What are the questions to be answered

- Where did the money go?
- What site did the victim go to?
- Who do you subpoena?
- What addresses belong to the suspect?
- Has law enforcement been contacted? - some law enforcement agencies have the resources to conduct their own crypto investigations.

Step 3 – Analysis (Tracing)

Use taint analysis - Technique used in cryptocurrency investigations to trace the flow of funds on a blockchain. It helps investigators understand the movement of potentially illicit or suspicious cryptocurrency by "tainting" specific coins or tokens and tracking them as they move across different addresses and transactions

There is no standard on tracing at this time. The tracing methodology used **should be the method used by law enforcement agencies where the victim is located.**

Different methodologies to tracing –

a. Last In First Out (LIFO)
b. First In First Out (FIFO). Used by the FBI
c. Specific Identification
d. PIFO (Illicit Proceeds First In First Out)

Choose a methodology and be consistent – **Do not switch methods because it is convenient.**

Step 4: Reporting

- Include background info on the scam itself
- Conclusions as to what happened. Answer where the money went
- Show exchange addresses
- Show deposit wallet and hot wallet addresses

- Provide a detailed path explanation of how each transaction occurred, eg. Each wallet used.
- Visualizations – Use pictures and images

Step 5: Communicate Results to the Client

- Delivery of reporting for victim reference.
- List of applicable agencies the victim can further report to.
- Reaffirm healthy expectations client should have, alongside helpful tips in communicating with law enforcement concerning updates to their case.

Contributors

CoinStructive

Breadcrumbs

Build Your Blocks Inc.